微软最有价值的专家

王春海最新力作

Windows Server 2008 R2 系统管理实战

王春海　薄鹏　编著

一册在手 全面掌握

- 微软MCSA、MCSE、MCITP认证考试最佳实用参考书
- 全面掌握Windows Server 2008 R2系统管理相关知识
- 以实践应用为主，以理论讲解为辅
- 精心设计所有应用场景和案例
- 适合Windows系统管理员和网络管理维护人员

清华大学出版社

Windows Server 2008 R2 系统管理实战

王春海　薄鹏　编著

清华大学出版社
北　京

内 容 简 介

Windows Server 2008 R2 是 Microsoft 最新一代的服务器操作系统，功能十分丰富，可以用来构建可靠、灵活的服务器基础结构。现在许多单位的网络仍然是 Windows Server 2003/2008，这些企业会面临从 Windows Server 2003 或 Windows Server 2008 升级到 Windows Server 2008 R2 的问题。本书选择企业关心的问题进行介绍，并通过设计多个场景让企业对升级的过程进行模拟与测试，让网络管理员学会并掌握这些内容，以管理最新的 Windows Server 2008 R2 网络。

本书内容翔实，结构清晰，以实践应用为主、理论为辅，全面系统地介绍了 Windows Server 2008 R2 系统管理、网络维护和网络应用的解决方案。

本书适合作为 Windows Server 2008 R2 系统管理员和网络维护人员阅读，也可供从事网络维护与系统集成工作的读者参考，还可以作为各大中专院校相关专业的教材。另外，本书对于正从事 Windows 网络组建、网络管理、网络应用的工作人员提高技术水平，增加组网经验有极大帮助。

图书在版编目（CIP）数据

Windows Server 2008 R2 系统管理实战 / 王春海，薄鹏编著. —北京：清华大学出版社，2012.1

ISBN 978-7-302-27309-7

I.① W…　II.① 王…　② 薄…　III.①服务器—操作系统（软件），Windows Server 2008　IV. ①TP316.86

中国版本图书馆 CIP 数据核字（2011）第 235253 号

责任编辑：夏非彼
责任校对：闫秀华
责任印制：王秀菊
出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　销：全国新华书店
开　本：190×260　**印　张**：37　**字　数**：947 千字
版　次：2012 年 1 月第 1 版　**印　次**：2012 年 1 月第 1 次印刷
印　数：1~4000
定　价：69.00 元

产品编号：043224-01

前　　言

Windows Server 2008 R2 是目前 Microsoft 最新的服务器操作系统，功能相当丰富。本书介绍适合管理中国国情的 Windows 网络所必需的一些服务，例如 DNS、DHCP、WINS、WSUS、共享文件夹、远程管理等。本书不仅适合读者入门、还可以快速提高读者使用 Windows Server 2008 R2 管理网络的能力及水平，笔者还将多年来管理、使用 Windows Server 网络中碰到的一些问题及经验倾囊相授，让读者在管理、升级与维护 Windows 网络的过程中少走弯路。

本书内容

本书全面系统地为 Windows Server 2008 R2 系统管理员提供系统管理和网络维护、网络应用的解决方案，本书共有 16 章，具体内容安排如下：

第 1 章， Windows Server 2008 R2 系统管理概述，介绍 Windows 产品的划分与命名、Windows Server 2008 R2 组件的组成、在网络中选择合适的 Windows Server 2008 产品与版本，还介绍了怎样学好 Windows Server 2008 R2 的“三步曲”，最后介绍在虚拟机中安装 Windows Server 2008 R2 的内容。

第 2 章，Windows Server 2008 R2 基本配置，介绍 Windows Server 2008 R2 的基本操作，例如修改 IP 地址、修改计算机名称、Windows Server 中“多网络设置”、Windows 防火墙设置、系统任务、设备管理器等，还介绍“本地用户和组”的管理等内容。

第 3 章，基本网络服务，介绍 Windows 网络中的“三大基本网络服务”，即 DNS、DHCP、WINS 服务器的基本知识。

第 4 章，磁盘与文件系统管理，介绍磁盘与存储的关系、RAID5 基础知识、NTFS 文件系统等，介绍磁盘与卷管理、在 Windows Server 2008 R2 中创建镜像卷、RAID5 卷、NTFS 权限、NTFS 压缩与加密、BitLocker 驱动器加密、磁盘配额、文件夹配额与文件屏幕、文件和打印机共享、卷影副本等内容。

第 5 章，Internet 信息服务器管理与应用，介绍 Web 服务器与 FTP 服务器的管理与应用内容，还介绍最新的 Windows Server 2008 R2 的 FTP 服务器支持双线 WAN 的配置方法。

第 6 章，Microsoft 系统更新服务器 WSUS 服务器的内容，介绍 WSUS 的安装、配置与管理，以及 WSUS 的常见故障及解决方法。

第 7 章，Active Directory 网络管理，介绍 Windows Server 2008 R2 中 Active Directory 网络规划，Active Directory 用户与用户组管理，以及将 Windows XP、Windows 7 计算机加入到域，使用 Windows 7 远程管理 Windows Server 2008 R2 的内容。

第 8 章，使用组策略管理网络，介绍组策略基础、使用组策略定制用户的环境、使用组策略发布软件，包括发布 Office 2003、Office 2010 的内容。还介绍了最新的 Windows Server 2008 R2 中“首选项”的使用。

第 9 章，使用 RMS 保护企业内部的 Office 文档，介绍使用 Microsoft RMS 保护企业内部资料不被窃取的内容。使用 RMS，可以让指定的用户、在指定的时间（以服务器时间为准）以及指定的时间范围内、以指定的行为（只读、不允许复制、不允许打印等）查看指定的文档。即使非授权用户非法复制受保护的文档，也不能打开并查看其内容。

第 10 章，DFS 分布式文件系统管理与应用，介绍 Windows Server 2008、Windows Server 2008 R2 中的分布式文件系统的应用。

第 11 章，Hyper-V Server 2008 虚拟化产品配置、应用与管理，介绍 Microsoft 服务器虚拟化的产品 Hyper-V 的应用，包括 Hyper-V 的选择、安装配置、Hyper-V 基础知识，在 Hyper-V 中创建虚拟机、创建模板虚拟机、在虚拟机中安装操作系统、导出导入虚拟机、差异磁盘等内容。

第 12 章，使用 SCVMM2008 R2 管理 Hyper-V，介绍 Microsoft 专用虚拟机管理工具 SCVMM 2008 R2 管理 Hyper-V 的内容，包括 SCVMM 2008 R2 的安装配置、共享服务器与库共享资源、使用 VMM 在 Hyper-V 中创建虚拟机、在虚拟机中安装操作系统、创建虚拟机的模板与模板使用、虚拟机的迁移等。

第 13 章， Windows Server 2008 R2 终端虚拟化应用，介绍 Windows Server 2008 R2 的终端虚拟化的基础知识、安装用于终端虚拟化的程序、发布 RemoteApp 应用程序等。使用终端虚拟化，可以解决企业工作站频繁升级的问题。

第 14 章，从 Windows Server 2003 升级到 Windows Server 2008 R2，介绍怎样从现有的 Windows Server 2003 网络升级到最新的 Windows Server 2008 R2 的内容，包括 Active Directory、DHCP 的升级，以及从 ISA Server 2006 升级到 Forefront TMG 2010 等内容。

第 15 章，使用网络为工作站部署操作系统，介绍使用 Windows 部署服务，通过网络为工作站安装、部署 Windows Vista、Windows 7、Windows Server 2008、Windows Server 2008 R2 的内容。

第 16 章，Forefront TMG 2010 系统管理与应用，介绍 Microsoft 最新的集防火墙、代理服务器、入侵检测于一身的安全软件 Forefront Threat Management Gateway 2010 的内容，包括 Forefront TMG 的安装、配置、防火墙策略、发布服务器，以及使用 Forefront TMG 组建 SSTP、PPTP 与 L2TP 的 VPN 服务器、VPN 路由的内容。在本节中，还介绍了 Windows Server 2008 R2 证书服务的配置与应用等内容。

本书的学习原则

尽管写本书时，编者精心设计了每个场景、案例，已经考虑到一些相关企业的共性问题，但是，就像天下没有完全相同的两个人一样，每个企业都有自己的特点和需求。所以，这些案例可能并不能完全适合你的企业，在实际应用时需要根据企业的情况进行改动。

技术类的图书，有时候看一遍可能会看不懂，这不要紧，只要多想想，多看几遍可能就明白了。技术，尤其是专业的技术，相对来说比较枯燥。所以，有时候需要多次阅读、思考，并反复进行实验，直到学会每个知识。

本书很好地利用了插图进行详细的产品使用解说，为系统管理人员提供了可以按部就班进行参照的工作手册。所以，我们推荐读者采用如下方式进行学习：

- 照做实验，关键是计算机的名称、IP 地址、子网掩码、DNS 设置等。

- 自己修改关键数据（计算机名称、IP 地址、DNS 域名等），再做实验。
- 将实验环境改造，用于实际工作环境。
- 使用注意事项、备份策略、做记录等。

作者简介

本书作者王春海，1993 年开始学习计算机，1995 年开始从事网络方面的工作，1996 年开始使用 Windows NT Server 3.51 组建全省国税系统的网络，其后亲历了 Microsoft 每个产品测试版到正式版的使用、升级与维护，直到现在的 Windows Server 2008 R2。作者一直维护与管理 Windows 网络，期间积累了大量的经验与心得，这些都穿插在书中。

本书作者在网络应用、网络组建、网络安全、虚拟机技术等多个方面都有很深的研究，精通 Microsoft 的 ISA Server、Forefront TMG、Windows Server 2003、Windows Server 2008、SharePoint、Exchange 等多个方面的产品，是 2009 年度 Microsoft Management Infrastructure 方面的 MVP（微软最有价值专家）、2010～2011 年度 Microsoft Forefront（ISA Server）MVP。

作者曾经主持组建过省国税、地税、市铁路分局（全省范围）的广域网组网工作，近几年一直从事政府等单位的网络升级、改造与维护工作，参与了多家政府、企事业单位组建并维护包括 Windows、Linux 网络在内的多种网络，在长期的工作中积累了大量的经验并解决了许多问题。

本书主要由王春海、薄鹏编写，盖俊飞、赵艳、张丽荣、高红玮、朱淑敏、任文霞、杜卫国、马卫华、曹志霞、包磊、贾启海、韩山峰、杨成才、周延雄、卢松波、张超等人也编写了本书的部分内容。

由于编者水平有限，并且本书涉及的系统与知识点很多，尽管笔者力求完善，但仍难免有不妥和错误之处，诚恳地期望广大读者和各位专家不吝指教。有关本书的意见反馈和更新消息以及读者在学习中遇到的问题，可以通过下列方式与作者联系。

作者个人网站：http://www.wangchunhai.cn

51cto 专家博客：http://wangchunhai.blog.51cto.com

电子邮件：wangchunhai@wangchunhai.cn

因为笔者在网络、虚拟机、数据恢复方面出版了多本图书，所以，在您给我发送邮件时，请写清您阅读的是我写的哪一本书、在学习哪一章时碰到了那样的问题，并且介绍您当前的实验（或生产）环境，最好是将错误截图附在文档中，您提供的信息越多、越详细，我能提供的帮助会越准确、越及时。

王春海

2011 年 10 月

目　　录

第 1 篇　基础服务配置管理与应用

第 2 篇 Active Directory 网络管理与应用

第 3 篇 Microsoft 云计算应用平台与管理

第 1 篇

基础服务配置管理与应用



第 1 章　Windows Server 2008 R2 系统管理概述

许多人经常问我，Windows Server 2008 R2 有什么用？能干什么？有什么好外？它与 Windows XP、Windows 7 有什么区别？也有的人说，我现在的系统是 Windows Server 2003，感觉就已经很好了，用不着 Windows Server 2008 R2。Windows Server 2008 R2 是不是对服务器的要求很高？学习是不是很难呢？我能不能学会呀？还有人说，我已经会安装 Windows Server 2008 R2 了，大部分功能也差不多理解了，但这些怎么用呢？在什么地方什么时候用呢？作为本书的开篇之章，我们将逐一回答这些问题。

1.1　Microsoft 产品划分与命名

首先来介绍 Microsoft 产品的划分与命名原则。Microsoft 产品众多，包括“操作系统”、“服务器”、“应用程序”、“开发人员工具”、“设计人员工具”、“Business Solutions”等。

1.1.1　Microsoft 操作系统

Microsoft 操作系统包括 MS-DOS、Windows 3.x、Windows 95、Windows 98、Windows ME、Windows 2000、Windows XP、Windows Vista、Windows 7、Windows NT、Windows Server 2008、Windows Server 2008 R2、Windows Home Server、Windows Small Business Server、Windows Storage Server、Windows Essential Business Server、Windows CE 等产品。

我们经常听到“客户/服务器”系统或“C/S”系统，这里的 C 是 Client（工作站）的简称，S 是 Server（服务器）的简称。对于 Microsoft 操作系统来说，其产品划分为工作站与服务器两大类。例如，当前流行的 Windows XP、Windows 7 属于工作站操作系统，而 Windows Server 2003、Windows Server 2008、Windows Server 2008 R2 则属于服务器操作系统。

对于每个操作系统来说，由于对用户的定位不同，还可能会有多个版本。例如，Windows XP 包括 Windows XP Professional（专业版）、Windows XP Home（家庭版）、Windows XP Media Center Edition（专门为个人电脑使用的媒体中心版本）、Windows XP Tablet PC Edition（为平板可旋转式的笔记本电脑 Tablet PC 设计的版本）、Windows XP Embedded（嵌入式版本）。另外，对于 Windows XP 来说，还包括 Windows XP Professional N 和 Windows XP Home Edition N 版本，这是微软公司根据欧盟的裁决在欧盟成员国发布的不带 Windows Media Player 的 Windows XP 版本。Windows XP Professional 还分 32 位与 64 位版本。

对于当前最流行的个人（工作站）操作系统 Windows 7，包括 Windows 7 Starter（简易版）、Windows 7 Home Basic（家庭普通版）、Windows 7 Home Premium（家庭高级版）、Windows 7 Professional（专业版）、Windows 7 Enterprise（企业版）、Windows 7 Ultimate（旗舰版）6 个版本，其中除了 Windows 7 Starter 只有 32 位版本外，其他产品还分 32 位与 64 位版本。Windows 7 Starter、Windows 7 Home Basic、Windows 7 Home Premium 适合家庭或个人用户使用，如果是在企业使用，则需要使用 Windows 7 Professional、Windows 7 Enterprise、Windows 7 Ultimate 版本。

Windows Server 2003 有 Web 版、Standard（标准版）、Enterprise（企业版）、Datacenter（数据中心版），其中标准版、企业版、数据中心版都有 32 位与 64 位版本。Windows Server 2003 各版本的区别如下：

- Windows Server 2003 Web 版用于构建和存放 Web 应用程序、网页和 XML Web Services。它主要使用 IIS 6.0 Web 服务器并提供快速开发和部署使用 ASP.NET 技术的 XML Web Services 和应用程序。支持双处理器，最低支持 256MB 的内存，最高支持 2GB 的内存。
- Windows Server 2003 标准版的销售目标是中小型企业，支持文件和打印机共享，提供安全的 Internet 连接，允许集中的应用程序部署。它支持 4 个处理器，最低支持 256MB 的内存，最高支持 4GB 的内存。
- Windows Server 2003 企业版支持高性能服务器，并且可以群集服务器，以便处理更大的负荷。通过这些功能实现了可靠性，有助于确保系统即使在出现问题时仍可用。在一个系统或分区中最多支持 8 个处理器，8 节点群集，最高支持 32GB 的内存。
- Windows Server 2003 数据中心版是针对要求最高级别的可伸缩性、可用性和可靠性的大型企业或国家机构等设计的。32 位版本支持 32 个处理器，支持 8 节点集群；最低要求 128MB 内存，最高支持 512GB 的内存。64 位版本支持 Itanium 和 Itanium2 两种处理器，支持 64 个处理器，支持 8 节点集群，最低支持 1GB 的内存，最高支持 512GB 的内存。

Windows Server 2003 R2 是在 Windows Server 2003 SP1 的基础上，添加“活动目录应用模式（ADAM）”、SharePoint 2、活动目录联合服务（ADFS，也称为 TrustBridge），修正了“分布式文件系统复制功能”等组件而来的。Windows Server 2003 R2 包括两张安装盘，其第 1 张安装与 Windows Server 2003 With SP1 完全一样，第 2 张安装盘包括 Windows Server 2003 R2 的产品组件。Windows Server 2003 与 Windows Server 2003 R2 的序列号生成算法不同，在使用 Windows Server 2003 安装程序时根据不同的序列号选择不同的版本。Windows Server 2003 SP1（SP2）很容易升级到 Windows Server 2003 R2，只要从 Windows Server 2003 R2 的第二张安装盘运行安装程序，输入 Windows Server 2003 R2 的序列号，就可以升级到 Windows Server 2003 R2。

Windows Server 2003 与 Windows XP 具有相同的内核。

Windows Server 2008 与 Windows Server 2008 R2 包括 Web 版、标准版、企业版和数据中心版，其中 Windows Server 2008 的每个版本都有对应的 32 位与 64 位版本，而 Windows Server 2008 R2 只有 64 位版本。Windows Server 2008 与 Windows Vista 具有相同的内核，而 Windows Server 2008 R2 与 Windows 7 有相同的内核。

相比 Windows Server 2003，Windows Server 2008 最大的改进有两点：Server Core 与 Hyper-V。其中，Server Core（服务器内核）提供一个最小化的 Windows Server 2008 环境，没有图形界面，

只有文本界面，可以降低系统维护与管理要求、减少使用硬盘容量、降低被攻击风险。而 Hyper-V 是 Microsoft 的虚拟机技术，相比 Microsoft Virtual PC、Microsoft Virtual Server 2005，它具有更高的性能和吞吐量。

Windows Home Server 是家用服务器操作系统，它支持文件共享、自动备份、远程访问、卷影副本等功能。

Windows Storage Server 是基于 Windows Server 2003 或 Windows Server 2008、Windows Server 2008 R2 的专用文件和打印服务器。Windows Storage Server 是具有强大存储软件运算能力、与各种不同存储硬件设备连接能力的存储服务器产品，它能够满足企业对磁盘阵列、服务器及异构网络环境等不同存储解决方案的需求。Windows Storage Server 只能通过与 Microsoft 公司合作的 OEM 厂商提供软硬件集成的网络存储产品，不单独销售软件光盘。

Windows Small Business Server 为小型企业提供了一个服务器产品集成包，最多支持 75 个用户或设备，包括电子邮件、安全的 Internet 连接、企业 Intranet、远程连接、移动设备支持、文件和打印机共享、备份和还原功能，以及用于协作的应用程序平台。它是以 Windows Server 2003（或 Windows Server 2008）为基础，集成了 Microsoft Windows SharePoint Services、Exchange Server、Office Outlook、SQL Server 等 Server 类产品的安装包。

Windows Essential Business Server 是为中型企业设计的服务器解决方案，最多支持 300 个用户或设备。Windows Essential Business Server 基于 Windows Server 2008，它有标准版和高级版两个版本。标准版包括三个安装了 Microsoft Exchange Server 2007、Microsoft System Center Essentials、Microsoft Forefront Security for Exchange Server 和 Forefront Threat Management Gateway 的标准版 Windows Server 2008。高级版在标准版的基础上增加了一个标准版 Windows Server 2008 和一个标准版 Microsoft SQL Server 2008。

所以，Windows Small Business Server 与 Windows Essential Business Server，都是 Windows Server 2003（或 Windows Server 2008、Windows Server 2008 R2），集成了 Exchange Server、SQL Server 等产品的工具包。

1.1.2　服务器

Microsoft 的 Server 类产品众多，包括应用程序虚拟化平台 Application Virtualization、BizTalk Server、Commerce Server、微软企业桌面优化套件 Desktop Optimization Pack、邮件服务器产品 Exchange Server、即时消息与视频会议产品 Office Communications Server 2007、Lync Server 2010、防火墙与代理服务器产品 Microsoft ISA Server、Forefront Threat Management Gateway（TMG）2010、企业门户网站 SharePoint Server、数据库服务器 SQL Server、系统管理工具 System Center Operations Manager、虚拟机管理产品 System Center Virtual Machine Manager、Windows MultiPoint Server 2011（类似 BetWin 的软件，可以让一台 PC 带多个键盘、鼠标、显示器充当多个主机来用）等产品。

1.1.3　应用程序

Microsoft 应用程序的产品包括：Microsoft Office 系列（Word、Excel、PowerPoint、Access）、OneNote、项目管理软件 Project、Publisher、画图软件 Visio、虚拟机软件 Microsoft Virtual PC 与

Virtual Server 2005、网站编辑软件 SharePoint Designer 与 FrontPage、InfoPath、主机虚拟化产品 Hyper-V Server 2008 与 Hyper-V Server 2008 R2、Internet Explorer、MapPoint 等。

1.1.4　其他分类

Microsoft 的“开发人员工具”包括 Visual Basic、Visual C++、Visual FoxPro、Visual Studio、Windows Embedded 等。

Microsoft 的“设计人员工具”包括 AutoCollage 2008、Songsmith、Expression Studio 等产品。

Microsoft 的 Business Solutions 主要包括 Dynamics CRM、Dynamics Point of Sale 2009、Small Business Manager Financials、Solomon。

1.2　Windows Server 2008 R2 的组件

Windows Server 2008 R2 是一个基础服务平台，它包括一系列只能在这个“基础服务”平台运行的功能包（也称为组件），用户可以根据自己的情况、选择适合自己的组件，以获得所需要的服务。Windows Server 2008 R2 提供了如下的组件：

（1）Internet 信息服务（IIS）：主要包括 Web 与 FTP 服务器。 其中，Windows Server 2008 提供了 IIS 7.0，Windows Server 2008 R2 提供了 IIS 7.5。

（2）文件服务器。许多人最早接触“客户/服务器”系统，就是通过类似“共享文件夹”提供的文件和打印机共享开始的，所以，许多人眼中的服务器，就是提供“文件夹”共享的服务器。在 Windows Server 2008 R2 中，文件服务器在网络上提供一个中心位置，用户可以在其中存储文件以及与网络中的用户共享文件。当用户要求某个重要文件（如项目计划）可由多个用户访问时，他们可以远程访问文件服务器上的文件，而不必在各自的计算机之间传送该文件。

Windows Server 2008 R2 的文件服务器包括下列角色：

- 共享和存储管理。
- 分布式文件系统（DFS）。
- 文件服务器资源管理器（FSRM）。
- 网络文件系统（NFS）服务。
- Windows 搜索服务。
- Windows Server 2003 文件服务。

（3）DHCP 服务器。DHCP 是一种客户端/服务器技术，它允许 DHCP 服务器将 IP 地址分配给作为 DHCP 客户端启用的计算机和其他设备，也允许服务器租用 IP 地址。使用 DHCP，可以实现以下功能：

- 在特定的时间内将 IP 地址租用给 DHCP 客户端，然后当客户端请求续订时自动续订 IP 地址。
- 通过更改 DHCP 服务器处的服务器或作用域选项，而不是在所有 DHCP 客户端上分别执

行此操作，来更新 DHCP 客户端参数。

- 为特定的计算机或其他设备保留 IP 地址，以便它们总是具有相同的 IP 地址，同时还接收最新的 DHCP 选项。
- 从 DHCP 服务器分发中排除 IP 地址或地址范围，以便能够使用这些 IP 地址和范围对服务器、路由器和其他需要静态 IP 地址的设备进行静态配置。
- 为众多子网提供 DHCP 服务(如果 DHCP 服务器和需要提供服务的子网之间的所有路由器都被配置成转发 DHCP 消息）。
- 配置 DHCP 服务器以便为 DHCP 客户端执行 DNS 名称注册服务。
- 为基于 IP 的 DHCP 客户端提供多播地址分配。

（4）DNS 服务器。通过使用域名系统（DNS）服务器角色，可以为网络上的用户提供主要名称解析过程。名称解析过程使用户能够利用计算机名称而不是 IP 地址来查找网络上的计算机。运行 DNS 服务器角色的计算机可以承载分布式 DNS 数据库的记录，并且可以使用这些记录来解析由 DNS 客户端计算机发送的 DNS 名称查询。这些查询可以包括网络或 Internet 上诸如 Web 站点或计算机名称的请求。

（5）WINS 服务器。DNS 服务器是将 DNS 名称解析为 IP 地址的服务，而 WINS 服务器是将 NetBIOS 名称解析为 IP 地址的服务。在具有 VLAN 的网络中，需要使用 NetBIOS 名称时，就需要使用 WINS 服务器。

（6）Windows 部署服务。Windows Server 2008 R2 中的“Windows 部署服务”角色是在 Windows Server 2003 的“远程安装服务(RIS)”基础上经过重新设计的更新版本。可以使用 Windows 部署服务通过网络来部署 Windows 操作系统（特别是 Windows Vista、Windows 7 和 Windows Server 2008 以及 Windows Server 2008 R2）。可以使用 Windows 部署服务角色，通过基于网络的安装来安装新计算机。这意味着用户不必亲自操作每台计算机，也不必直接通过 CD 或 DVD 安装每个操作系统。

（7）打印服务。使用打印服务，可以在网络上共享打印机，也可以使用“打印管理”单元集中执行打印服务器和网络打印机管理的任务。这有助于监视打印队列，并在打印队列停止处理打印作业时接收通知。此外，该服务还可以使用“组策略”来迁移打印服务器并部署打印机连接。

（8）网络策略和访问服务。“网络策略和访问服务”是在 Windows Server 2003 的“路由和远程访问服务器”的基础上，经过重新设计的更新版本。网络策略和访问服务提供以下网络连接解决方案：

- 网络访问保护（NAP）。NAP 是一种创建、强制和修正客户端健康策略的技术，包含在 Windows Vista、Windows 7 客户端操作系统和 Windows Server 2008、Windows Server 2008 R2 操作系统中。通过 NAP，系统管理员可以设置并自动强制运行状况策略，策略中可以包含软件要求、安全更新要求、计算机配置要求以及其他设置。可以为不符合健康策略的客户端计算机提供受限网络访问，直到更新其配置并且使其符合策略时为止。根据选择部署 NAP 的方式，可以自动更新不兼容的客户端，使用户可以快速重新获得完全的网络访问，而不必手动更新或重新配置其计算机。
- 安全无线与有线访问。在部署 802.1X 无线访问点时，安全无线访问会向无线用户提供一

种易于部署的、基于密码的安全身份验证方法。当部署 802.1X 身份验证切换时，有线访问可以确保 Intranet 用户通过身份验证后才可以连接到网络或使用 DHCP 获取 IP 地址，从而保护网络安全。

- 远程访问解决方案。使用远程访问解决方案，可以向用户提供对你组织的网络的虚拟专用网（VPN）和拨号访问权限。还可以通过 VPN 解决方案将分支机构连接到你的网络，在你的网络上部署功能齐全的软件路由器，并在整个 Intranet 中共享 Internet 连接。
- 使用 RADIUS 服务器和代理进行的集中网络策略管理。无须在无线访问点、802.1X 身份验证切换、VPN 服务器和拨号服务器等每台网络访问器上配置网络访问策略，只需在一个位置创建策略，即可指定网络连接请求的所有方面内容，包括允许谁进行连接，他们何时可以连接，以及连接到网络时必须要使用的安全等级。

（9）Hyper-V。通过 Hyper-V，可以使用 Windows Server 2008 R2 中的虚拟技术创建一个虚拟化的服务器计算环境。利用虚拟化计算环境，以及多个硬件资源来提高计算资源的效率。Hyper-V 提供 Windows Server 2008 R2 中的软件基础结构和基本的管理工具，可用于创建和管理虚拟化服务器计算环境。此虚拟化环境可用来实现提高效率和降低成本的各种商业目标，具体如下：

- 通过提高硬件的利用率，降低运行和维护物理服务器的成本，以减少运行服务器负载所需的硬件数量。
- 通过减少设置硬件、软件以及在线测试环境所需的时间以提高开发和测试效率。
- 提高服务器可用性，通过使用负载平衡系统故障转移集群提供持续不断的服务并保证服务可访问。

（10）Active Directory 域服务。利用 Windows Server 2008 R2 操作系统中的 Active Directory 域服务（AD DS）服务器角色，可以创建用于用户和资源管理的可伸缩、可管理及安全的基础结构，并且可以提供对启用目录应用程序（如 Microsoft Exchange Server、Microsoft SharePoint Server、LYNC 2010）的支持。Active Directory 域服务的核心是 AD DS 服务器角色。AD DS 提供分布式数据库，该数据库存储和管理有关网络资源和来自支持目录的应用程序的特定数据。管理员可以使用 AD DS 将网络元素（如用户、计算机和其他设备）整理到层次内嵌结构。层次内嵌结构包括 Active Directory 林、林中的域以及每个域中的组织单位（OU）。运行 AD DS 的服务器称为域控制器。

简单来说，Active Directory 在网络中提供了一个统一的身份验证、身份认证平台，所有基于 Microsoft Active Directory 的产品，如 Exchange Server、SharePoint Server 等，都采用这个平台进行于统一的身份验证。

（11）Active Directory 证书服务。Windows Server 2008 中的“Active Directory 证书服务”，是在原来 Windows Server 2003 的“证书服务”的基础上的升级、改进版本。Active Directory 证书服务仍然包括“企业证书服务器”与“独立证书服务器”。

（12）Active Directory Rights Management Services。Active Directory Rights Management Services（简称 RMS）以前是一个单独的产品，从 Windows Server 2008 开始集成在操作系统中。简单来说，RMS 是 Microsoft 的“权限管理服务器”，用来在企业网络中保护 Office 文档，它可以

让指定的用户（Active Directory 用户）在指定的时间内以指定的权限（读、写、是否打印、是否具有“复制”权限）访问受保护的文档。如果用户转发受保护的文档（例如通过电子邮件）给不具有访问权限的用户，受限用户也不能打开。

（13）终端服务器。通过 Windows Server 2008 R2 中的“终端服务”服务器角色提供的技术，用户可以访问终端服务器上安装的基于 Windows 的程序或访问完整的 Windows 桌面。使用终端服务，用户可以在企业网络内部或通过 Internet 访问终端服务器。

终端服务可使你在企业环境中有效地部署和维护软件，可以很容易从中心位置部署程序。由于将程序安装在终端服务器上，而不是客户端计算机上，所以，更容易升级和维护程序。

用户访问终端服务器上的某个程序时，该程序的执行在服务器上进行，只有键盘、鼠标和显示器的信息才能通过网络传输。每个用户只能看到自己的会话。服务器操作系统透明地管理会话，与任何其他客户端会话无关。

1.3　为什么要选择 Windows Server 2008

看了上面的介绍后，大家可能会说，Windows Server 2008 也没有什么新功能呀。即使有的新功能，在 Windows Server 2003 中也有对应的产品或组件，那么，为什么要选择 Windows Server 2008 呢？选择 Windows Server 2008 的理由如下：

（1）服务器整合与资源优化 —— Hyper-V

大多数服务器在工作时都远未发挥出自身应有的能力。平均而言，未得到利用的处理能力高达 80% ～ 90%。凭借 Windows Server 2008 虚拟化解决方案 Hyper-V，单个物理服务器就能支持多个业务系统（Line of Business）上的工作负载。Hyper-V 能帮助企业优化使用硬件资源，并提供足够的灵活性来充分满足不断变化的 IT 需求。新型管理工具可简化部署过程，并使 IT 部门能够像管理网络中物理服务器一样通过熟悉的工具来管理虚拟服务器。

（2）最简化的模块化安装——服务器核心（Server Core）

众多网络服务器都可能在网络中执行特定的应用或者担任某些关键的角色。全新的服务器核心安装选项可为运行这些特定应用的服务器或服务器角色提供最简化的环境，从而有助于提高可靠性与效率，使 IT 部门能更好地利用现有硬件。此外，也可以通过减少对不必要的文件和功能的更新或打补丁来简化持续的管理与补丁管理要求。 对于执行特定网络基础架构角色的网络服务器而言，新型 Server Core 安装选项提供了一种高度可靠的高效率平台。由于 Server Core 能够加载运行核心基础架构角色服务器所需的最少的操作系统组件，因而可以有效减少补丁需求，进而也提高了核心网络基础架构服务器的可靠性与安全性。

（3）只读域控制器（Read-only Domain Controller，RODC）

RDOC 是新型的域控制器，其数据库只能读取，不能修改，而且只能从其他可写的域外控制器上复制过来。在 Windows Server 2008 发布之前，如果用户必须通过广域网（WAN）对域控制器进行身份验证，则没有合适的替代方案。在很多情况下，分公司通常不能为可写域控制器提供所需的充分的物理安全性。此外，当分支机构连接到总公司时，其网络带宽状况通常较差，这可能增加登录所需的时间，还可能妨碍对网络资源的访问。

RODC 主要设计用于部署在远程或分支机构环境中。分支机构通常具有以下特性：

- 相对较少的用户。
- 物理安全性差。
- 到中心站点的网络带宽相对较差。
- 对信息技术（IT）的了解很少。

具备内置 Web 与虚拟化技术的 Microsoft Windows Server 2008 使企业能够大幅提升其服务器基础架构的可靠性与灵活性。全新的虚拟化工具、增强的 Web 资源管理及安全性功能不仅有助于节约时间、降低成本，同时还可为动态优化的数据中心提供平台。因特网信息服务（IIS）7.0 与服务器管理器（Server Manager）等功能强大的新型工具可提供更完备的服务器控制，并对 Web 配置以及管理任务等进行优化。诸如网络接入保护（Network Access Protection）与只读域控制器（RODC）等高级安全性和可靠性增强功能既能够提高操作系统的性能，而且还可确保服务器环境的安全，从而为商务运营打造一个坚实的基础。

（4）远程用户可灵活地存取应用——TS RemoteApp

Windows Server 2008 为终端服务（Terminal Services）带来了全面的性能改进与创新功能，其具备的 Terminal Services RemoteApp 等解决方案使用户能够访问单个独立的应用，而不是只在终端服务器（Terminal Server）会话中访问计算机桌面。这些应用运行于主计算机之上，仅负责向用户发送应用窗口，从而能够显著减少客户端所需要的资源，进而降低管理与部署成本。

（5）交付丰富的 Web 内容与应用 —— IIS 7.0

随着 Web 内容日益丰富而且其正成为提供商业应用的高效平台，Web 服务器也在向众多网络的核心发展。IIS 7.0 可为当今要求极高的内容提供解决方案，其中包括 ASP（Active Server Pages）与 PHP 中的流媒体和 Web 应用等。借助可简化管理工作的最新界面，采用全新模块化设计的 IIS 7.0 使管理员能够仅安装所需的组件，从而最大限度地缩小 Web 服务器的受攻击面。

（6）更高的网络性能与更完善的控制——新的 TCP/IP 协议栈

高效使用带宽会直接提高通过 WAN 连接至企业中央服务器上远程用户的工作效率。Windows Server 2008 采用经过精心设计的“新一代”TCP/IP，可大幅提升远程办公的性能，从而加快吞吐速率并能更高效地利用网络流量。通过在分支办公环境中结合采用 Windows Server 2008 与 Windows Vista，将有望把 WAN 连接的吞吐量提高两倍。

（7）避免不健康的设备连接至网络—— NAP

随着越来越多的移动用户和企业合作伙伴需要连接至企业组织机构的网络，这使得避免网络遭受外部威胁的工作始终面临着严峻的挑战。Windows Server 2008 中的网络接入保护（NAP）可阻止不符合规范的计算机接入企业网络。NAP 能够验证试图接入网络的计算机的健康状况，并确保让仅符合企业安全标准的设备成功接入。

（8）针对要求高的工作负载支持业务持续性——高可用性

Windows Server 2008 可为大多数要求最严格的商业解决方案提供更高的可扩展性，并能通过高可用性特性帮助企业应对意外停机事件。Windows Server 2008 支持故障恢复群集、网络负载平衡、动态硬件分区、稳健的存储选项以及高级机器自检架构等，可在单点故障问题情况下确保安全。简化的部署与管理工作还能帮助各种规模的组织机构充分发挥上述特性的优势，以显著提高可用性

与可靠性。

（9）实现安全协作——活动目录联合权限管理（Active Directory Federated Rights Management）

企业需要与合作伙伴和客户实现信息共享，同时又不能失去对该信息的控制。权限管理服务（Rights Management Service）使企业能够控制内外部使用文档的方式，其中包括哪些人可以查看文档，是否能够打印，能否转发或删除等。

（10）异构环境的互连

Windows Server 2008 包含的 UNIX 应用程序子系统（SUA）是一种多用户 UNIX 环境，能够支持超过 300 种 UNIX 命令、实用程序及外壳脚本等。用户可维护 Windows 域和 UNIX 系统的用户名和密码，在其中之一发生变化时实现证书的自动同步。SUA 运行在基于 Windows 的服务器上，无须任何仿真就能确保本机 UNIX 性能，并支持和充分发挥 Windows API 和组件优势的 UNIX 应用。

（11）支持 Top-Self Service 和远程站点

分支办公机构等远程站点可能会对 IT 工作提出挑战。分支部门通常没有自己的 IT 员工，这使得软件与安全更新的部署成本高昂、费时耗力，而且也很难在远程站点中严格实施安全与 IP 标准。Windows Server 2008 能让远程管理就像在物理总部办公一样，使管理人员能够通过远程管理技术纠正许多问题。全新的 RODC 为在远程基础架构中进行活动目录管理提供了一种更安全的途径。

（12）简化管理与自动化——Server Manager 和 PowerShell

服务器管理控制台（Server Manager Console）可为管理服务器的配置与系统信息提供单个统一的控制台，不仅可显示服务器的状态，明确服务器角色配置的问题，还能管理服务器上安装的所有角色。Server Manager 构建于服务建模语言（SML）平台之上，能够帮助管理人员用更少的点击次数完成各项任务，而无须在多种工具和接口间烦琐地切换。此外，Server Manager 还可直接与命令行外壳 PowerShell 接口相连，并支持脚本语言自动化。所有能在该接口中使用的 Server Manager 功能也都能应用于 PowerShell 脚本。该接口甚至还能帮助管理员编写脚本，向管理员准确显示每个按钮与控件背后到底是什么命令，而且还能让管理员记录 UI 中的任务执行，并将这些任务执行保存为脚本。

1.4 选择 Windows Server 2008 R2 的理由

Windows Server 2008 R2 是微软最新的 Windows 服务器操作系统软件，它是 Windows Server 2008 的升级版，具有所有 Windows Server 2008 的内容。Windows Server 2008 R2 的设计思想是增强对企业内资源的管理控制，提高工作效率以及减少操作的花销。Windows Server 2008 R2 更有效的能源利用率和更好的性能表现来源于降低能源的消耗率和较低的计算机总开销率。Windows Server 2008 R2 提供了更强的分支机构性能，令人兴奋的远程访问新体验，精简的服务器管理，并扩展了微软为服务器以及客户端计算机的虚拟化策略。

（1）强大的硬件和可扩展性

Windows Server 2008 R2 设计为在相同的硬件资源下提供和 Windows Server 2008 相同或者

更强的性能。另外，Windows Server 2008 R2 也是第一款仅有 64 位架构的 Windows 服务器操作系统。

Windows Server 2008 R2 对处理器进行了一些改进。首先，Windows Server 2008 R2 扩展了对处理器的支持，用户可以使用多达 256 个逻辑处理器。Windows Server 2008 R2 还支持 Second Level Address Translation（SLAT），以从最新的 ADM 处理器中的 Enhanced Page Tables 功能和最新的 Intel 处理器中的 Similar Nested Page Tables 功能中获得提升。这些方面的联用将使得 Windows Server 2008 R2 在运行时获得明显的内存管理提升。

Windows Server 2008 R2 的组件也获得了硬件支持方面的改进。现在 Windows Server 2008 R2 中的 Hyper-V 可以使用到高达 32wh 处理器的计算机上，这可是 Hyper-V 第一版支持处理器数量的两倍。这个方面的改进不但提高了对新的多核系统的利用，而且意味着单物理主机上更多的虚拟机共存比例。

（2）减少电源的消耗

Windows Server 2008 引入了一个叫做“平衡”的电源策略，它会监控服务器上的处理器使用率来动态调整处理器的性能状态，以减少工作负载所需的电源消耗。Windows Server 2008 R2 新加入的 Core Parking 功能和扩展的电源自适应组策略设置增强了节能功能。

Windows Server 2008 活动目录域服务组策略已经给管理员提供了大量针对客户端计算机的电源管理控制选项。在更多的部署场景中， Windows Server 2008 R2 和 Windows 7 中增强的节能设置可以提供比以往更精确的控制从而最大程度地减少能源消耗。

（3）Windows Server 2008 R2 的 Hyper-V

Windows Server 2008 R2 也包含了对 Microsoft 的虚拟化技术——Hyper-V 更有远虑的升级。新的 Hyper-V 针对扩大现有的虚拟机管理以及满足 IT 部门所遇到的挑战，尤其是服务器迁移这块的设计。

Hyper-V 可以使用 Windows Server 2008 R2 的一项内置功能——动态迁移。在 Windows Server 2008 的 Hyper-V V1 时代可以支持快速迁移功能，能够将虚拟机在物理主机之间迁移，而仅仅只有几秒钟的当机时间。不过，这几秒钟的时间也足够在特定的情境下引发问题，尤其是那些连接到虚拟主机服务器上的客户端。而到了动态迁移时代，虚拟机能够在几毫秒的时间内完成在物理主机之间迁移任务。也就是说，迁移操作对已连接用户来说是完全透明的了。

用户还可以部署针对 Hyper-V 开发的 System Center Virtual Machine Manager，它可以添加额外的管理选项以及管理方式，包括自适应的虚拟化性能和资源优化功能，以及针对故障还原群集管理的优化支持。

新的 Hyper-V 的核心性能增强还包括前文提到的支持最多 64 颗逻辑处理器，通过主机对 SLAT 的支持加强处理器方面的性能。最后，虚拟机可以添加和移除 VHD 磁盘而无须重启，甚至可以直接从 VHD 进行引导。

（4）VDI 减少了桌面花费

在服务器领域，虚拟化无疑是最热门的焦点。但是，同样令人激动的改进被加入到了表现层虚拟化中。表现层虚拟化是服务器端负责进程的处理；而图形界面、键盘、鼠标和其他的用户 I/O 操作则由用户的桌面发起。

Windows Server 2008 R2 包含了增强的虚拟化桌面集成（VDI）技术。VDI 技术扩展了终端服

务的功能，使得企业能够实现将某个业务软件投递到雇员远程桌面的需求。在 VDI 技术中，远程桌面服务将程序快捷方式发送到可用计算机的开始菜单中，运行起来和本地安装的软件没有区别。这种方式可以提供改进的桌面虚拟化功能以及更好的应用虚拟化。桌面虚拟化在 Windows 7 中，可以从改进的个性化管理、虚拟桌面和应用的无缝集成、更好的音频视频性能、非常酷的 Web 访问改进等等中获得益处。

虚拟化桌面集成（VDI）技术包含了更有效的使用虚拟化资源，更紧密的与本地外接硬件集成以及崭新强大的虚拟管理方面的功能。

（5）更简单、更有效的服务器管理能力

有这样一种说法：无论何时增加服务器操作系统的容量都是没错的。而对服务器管理员来说，操作系统的复杂程度越来越高，日常的工作负担也越来越大。Windows Server 2008 R2 特别针对这个问题，实现了自适应管理控制台，让其来接管大量的工作。这些工具的功能包括：

- 改进的数据中心能源消耗及其管理。
- 改进的远程管理功能，包括支持远程安装的 Server Manager。
- 改进的身份管理功能，升级并简化了活动目录域服务和活动目录联盟服务。

Windows Server 2008 R2 针对流行的 PowerShell 功能提供了改进。PowerShell 2.0 相比早期版本明显增强，包括超过 240 个新的脚本命令以及一个新的图形界面，并且添加了专业级别的脚本创建功能。新的图形界面包括语法颜色，新的脚本生成排错功能和新的测试工具。

（6）管理数据而不仅仅是管理磁盘

管理数据已经不再是管理磁盘了。在 2008 年到 2012 年间，互联网数据中心（IDC）拥有的存储卷将以每年 51%的速率增长。为了保持速度和竞争力，所有的组织都必须开始管理数据，而不仅仅是磁盘。Windows Server 2008 R2 为 IT 管理员提供了精确的管理工具——新的文件分类架构（FCI）。这个新功能在现有的共享文件架构之上，创建了一套可以扩展且自动化的分类方法。这个新功能使得 IT 管理员可以根据整体自定义分类方式直接针对某些文件进行某项操作。合作伙伴也可以扩展文件分类架构（FCI），也就是说在不远的将来，Windows Server 2008 R2 的用户可以看到来自于独立软件开发商围绕文件分类架构（FCI）开发的新功能。

（7）无所不在的远程访问

今天，要求 IT 部门为移动员工提供对企业资源远程访问要求的呼声日益高涨。然而，低速的广域网带宽，糟糕的连接效果，重复连接对冗长的桌面管理任务的干扰，比如组策略的修改、应用最新补丁等，面对这些问题如何管理远程计算机依然是一个持续的挑战。

Windows Server 2008 R2 引入了一项新的连接方式——Direct Access。Direct Access 是一种强大的无缝访问企业资源的方式，无须远程用户使用传统的 VPN 连接拨号或者客户端软件安装。在 Windows Server 2008 自带技术的基础上，微软增加了简单的管理向导，帮助管理员配置连接 Windows Server 2008 R2 和 Windows 7 客户端的 SSTP 和 IPv6 来实现基本的 DirectAccess 连接。并通过 Windows Server 2008 R2 上额外的管理和安全工具来扩展这种连接方式，比如管理策略和 NAP。

使用 DirectAccess 后，所有用户在任何时候都被认为是远程连接。用户无须区分本地连接和远程连接，所有的相关操作将由 DirectAccess 在后台处理。IT 管理员则保留了对这种连接双向的精确

访问控制以及完全的外围安全，并可减轻桌面的安全和管理带来的问题。

（8）改进的分支机构性能和管理性

许多分支机构的 IT 架构都或多或少会受低带宽的影响。低速的广域网连接导致分支机构雇员不得不等待程序从主机构获取信息，进而影响了分支机构雇员的生产力。而且所有分支机构的带宽花销差不多占了企业 IT 部门总开销的三分之一。为了迎接这个挑战，Windows Server 2008 R2 推出了新功能 BranchCache。BranchCache 可以减少广域网的使用并增强网络的反应速度。

使用 BranchCache 后，如果主机构的某个文件之前已经被读取过，那么下一个客户端对该数据的请求将直接发送到本地（分支机构）的网络中。大型分支机构的本地 BranchCache 服务器可以存储这些缓存下来的文件，当然也可以直接存放在本地 Windows 7 的计算机上。存储在本地的文件使得用户可以获得高速快捷的访问体验。

（9）中小型企业的简化管理性

在 Windows Server 2008 R2 上，微软对中小型企业用户也投入了越来越多的重视。这种重视体现在为这些用户提供了丰富的微软产品集，从 Small Business Server 到 Windows Essential Business Server 以及现在的 Windows Server 2008 Standard。所有这些产品都包含了简化中小型企业 IT 管理员的新管理工具。

所有的图形管理界面都基于 PowerShell，而且都集中在一个单独的图形界面中，比如活动目录新的 AD 管理中心就是一个例子。另外，微软为每个服务器角色都提供了最佳实践分析器，来帮助用户同步服务器配置，并了解发生了什么。最后，就是 Windows Server Backup 工具。这项内置的备份功能进行了非常大的改进，包括支持颗粒化的备份工作创建，对系统状态操作的支持，而且还进行了优化以实现更快的使用速度以及占用更少的磁盘空间。

（10）当今最强大的 Web 应用服务器

Windows Server 2008 R2 包含了大量的升级，不但使得它成为当今最佳的 Windows 服务器应用平台，同时更重要的一点就是最新的 IIS 7.5。

IIS 7.5 的升级包括扩展的 IIS 管理器带来的高效管理性，IIS 的 PowerShell 生成器的应用以及从 Server Core 支持.NET 获得的益处。IIS 7.5 还集成了新的支持和排错功能，包括配置日志记录和专门的最佳实践分析器。最后，IIS 7.5 还集成了一些在 Windows Server 2008 上的最佳可选扩展，比如 URLScan 3.0（或者称为请求筛选器模块）。

1.5 选择合适的产品与版本

通过前面的介绍，我们了解了 Windows Server 2008 与 Windows Server 2008 R2，并且了解到它们有众多的版本（Web 版、标准版、企业版、数据中心版、32 位与 64 位版本），那么，我们应该怎样选择这些版本呢？

1.5.1 全新安装系统的选择

如果是一个全新的网络，或者说，虽然一个网络已经被管理很长时间，但没有采用专门的 Windows Server 2003 或 Windows 2000 Server，则选择比较简单。

首先，来看服务器的配置。如果服务器是最近几年购买的并且是 64 位的 CPU，则优先选择 64 位版本的 Windows Server 2008 或 Windows Server 2008 R2。如果服务器购买得比较早，不是 64 位的 CPU，则只能选择 32 位的 Windows Server 2008。如果准备将新采购的服务器用于新建网络管理，则优先选择 Windows Server 2008 R2。

其次，根据所需要的功能进行选择。在不考虑升级的前提下，可根据需要的功能选择对应的版本。Windows Server 2008 R2、Windows Server 2008 的功能如表 1-1 所示。

表 1-1 Windows Server 2008 R2 各版本功能对比

功能	Web 版	标准版	企业版	数据中心版	Server Core
服务器角色					
Active Directory 证书服务	包含	包含	包含	包含	部分包含
管理员任务—Active Directory 域服务	不包含	包含	包含	包含	包含
只读域控制器—Active Directory 域服务（AD DS）	不包含	包含	包含	包含	包含
可重启 Active Directory—Active Directory 域服务	不包含	包含	包含	包含	包含
Active Directory 联合服务	不包含	不包含	包含	包含	不包含
Claims Aware 应用代理	不包含	不包含	包含	包含	不包含
Active Directory 轻量目录服务（AD LDS）	不包含	包含	包含	包含	包含
联合权限管理—Active Directory 权限管理服务（AD RMS）	不包含	不包含	包含	包含	不包含
应用服务器					
DHCP 服务器	包含	包含	包含	包含	包含
DHCP 服务器—群集 DHCP 服务器	不包含	包含	包含	包含	包含
DNS 服务器	不包含	包含	包含	包含	包含
传真服务器	不包含	包含	包含	包含	不包含
文件服务器	不包含	包含	包含	包含	不包含
文件服务器—Windows 搜索服务	不包含	包含	包含	包含	不包含
文件服务器—网络文件系统服务	不包含	包含	包含	包含	不包含
网络访问服务—网络策略服务器	不包含	包含	包含	包含	不包含
网络访问服务—远程访问服务	包含	包含	包含	包含	不包含
网络访问服务—安全注册部门	不包含	包含	包含	包含	不包含
网络访问服务—连接管理器管理工具包	包含	包含	包含	包含	不包含
网络访问服务—系统安全检验程序模板	不包含	包含	包含	包含	不包含
打印服务器	包含	包含	包含	包含	包含
打印服务器—导入与导出打印设置	包含	包含	包含	包含	包含
打印管理控制台	包含	包含	包含	包含	包含
终端服务	不包含	部分包含	包含	包含	不包含
终端服务网关	不包含	部分包含	包含	包含	不包含
终端服务 Remote App	不包含	部分包含	包含	包含	不包含
终端服务 Web 访问	不包含	部分包含	包含	包含	不包含
即插即用设备重定向（终端服务器）	不包含	部分包含	包含	包含	不包含
统一描述、发现与集成服务（UDDI）	不包含	包含	包含	包含	不包含
Web 服务器（Internet 信息服务-IIS）	包含	包含	包含	包含	包含
委托功能管理-IIS（包含 IIS6）	包含	包含	包含	包含	包含
Web 应用（Xcopy 部署 IIS）	包含	包含	包含	包含	包含
失败请求跟踪-IIS（包含 IIS6）	包含	包含	包含	包含	不包含
Windows 部署服务（WDS）	不包含	包含	包含	包含	包含

（续表）

功能	Web 版	标准版	企业版	数据中心版	Server Core
Windows 媒体服务（Media Server）	包含	包含	包含	包含	包含
Hyper-V（Windows 服务器虚拟化，需要 64 位版本）	不包含	包含	包含	包含	包含
服务器功能					
Windows 激活服务	不包含	包含	包含	包含	不包含
BITS 服务器扩展	不包含	包含	包含	包含	不包含
Windows Bitlocker 驱动器加密	包含	包含	包含	包含	包含
桌面体验包	包含	包含	包含	包含	不包含
高可用性功能					
故障切换群集	不包含	不包含	包含	包含	不包含
创建群集 API	不包含	不包含	包含	包含	不包含
群集迁移工具	不包含	不包含	包含	包含	不包含
多址群集	不包含	不包含	包含	包含	不包含
混合法定人数模板	不包含	不包含	包含	包含	不包含
恢复功能					
Windows 服务器备份	包含	包含	包含	包含	包含
裸机还原	包含	包含	包含	包含	包含
Internet 存储命名服务	包含	包含	包含	包含	不包含
LPR 端口监控	包含	包含	包含	包含	包含
MSMQ 服务	包含	包含	包含	包含	包含
Windows 网络负载均衡	包含	包含	包含	包含	不包含
远程协助	包含	包含	包含	包含	不包含
基于 HTTP 代理的 RPC	不包含	包含	包含	包含	不包含
可移动存储管理器	不包含	包含	包含	包含	不包含
SMTP 服务器	包含	包含	包含	包含	不包含
SNMP 服务	包含	包含	包含	包含	包含
SAN 存储管理器	不包含	包含	包含	包含	不包含
简单 TCP/IP 服务	包含	包含	包含	包含	包含
UNIX 应用子系统	包含	包含	包含	包含	包含
Telnet 客户端/服务器	包含	包含	包含	包含	包含
WINS 服务器	不包含	包含	包含	包含	包含
Windows 系统资源管理器	包含	包含	包含	包含	不包含
有条件资源分配策略	不包含	包含	包含	包含	不包含
SQL Server 账务引擎	不包含	包含	包含	包含	不包含
Microsoft .NET Framework 3.5	包含	包含	包含	包含	不包含
无线 LAN 服务	包含	包含	包含	包含	不包含
SQL Server（不包含 Embedded Edition）	包含	包含	包含	包含	不包含
事件浏览器					
事件浏览器	包含	包含	包含	包含	部分包含
Windows 事件收集服务	包含	包含	包含	包含	不包含
任务调度程序					
任务计划程序	包含	包含	包含	包含	不包含
文件系统与存储					
脱机客户端缓存	不包含	包含	包含	包含	不包含
存储浏览器	不包含	包含	包含	包含	不包含
事务文件与注册表操作	包含	包含	包含	包含	包含

（续表）

功能	Web 版	标准版	企业版	数据中心版	Server Core
按需文件复制	包含	包含	包含	包含	包含
iSCSI 启动程序	包含	包含	包含	包含	需要手动运行
分布式文件系统（DFS）	包含	包含	包含	包含	包含
组策略					
组策略	包含	包含	包含	包含	包含
组策略首选项	包含	包含	包含	包含	包含
硬件与设备					
硬件与设备（动态分区）	不包含	不包含	包含	包含	不包含
初始配置					
初始配置任务	包含	包含	包含	包含	不包含
微软管理控制台（MMC）					
微软管理控制台	包含	包含	包含	包含	不包含
性能与诊断程序					
性能与诊断程序	包含	包含	包含	包含	部分包含
Windows 内存诊断工具	包含	包含	包含	包含	包含
性能与可靠性监视器	包含	包含	包含	包含	部分包含
数据收集器集合（Perfmon）	包含	包含	包含	包含	部分包含
平台网络					
平台网络 IPv6	包含	包含	包含	包含	包含
平台网络接收端缩放	包含	包含	包含	包含	包含
企业 QoS（服务质量）	包含	包含	包含	包含	包含
安全套接字 API	包含	包含	包含	包含	包含
间隔网关保护	包含	包含	包含	包含	包含
Windows 过滤平台	包含	包含	包含	包含	包含
TCP 卸载	包含	包含	包含	包含	包含
接收窗口自动缩放	包含	包含	包含	包含	包含
黑洞路由器检测	包含	包含	包含	包含	包含
网络诊断框架	包含	包含	包含	包含	包含
平台安全性					
平台安全性	包含	包含	包含	包含	包含
高级安全 Windows 防火墙	包含	包含	包含	包含	包含
连接安全角色向导	包含	包含	包含	包含	不包含
Windows 服务强化	包含	包含	包含	包含	包含
设备安装控制台	包含	包含	包含	包含	包含
系统文件保护	包含	包含	包含	包含	包含
软件保护平台					
软件保护平台	包含	包含	包含	包含	包含
密钥管理服务	不包含	包含	包含	包含	不包含
精简功能模式	包含	包含	包含	包含	包含
服务器核心（Server Core）					
服务器核心	不包含	包含	包含	包含	包含
服务器管理器					
服务器管理器	包含	包含	包含	包含	不包含
更新服务	包含	包含	包含	包含	包含

（续表）

功能	Web 版	标准版	企业版	数据中心版	Server Core
添加任务向导	包含	包含	包含	包含	不包含
添加功能向导	包含	包含	包含	包含	不包含
Windows Management Instrumentation					
Windows 管理规范服务	包含	包含	包含	包含	包含
Windows PowerShell					
Windows PowerShell	包含	包含	包含	包含	不包含
Remote					
Windows 远程管理规范（WinRM）	包含	包含	包含	包含	包含
Windows Remote Shell（WinRS）	包含	包含	包含	包含	包含
授权管理器					
授权管理器	包含	包含	包含	包含	包含
UNIX 身份管理					
UNIX 身份管理	包含	包含	包含	包含	包含
事务					
分布式事务协调器	包含	包含	包含	包含	包含
内核事务管理器	包含	包含	包含	包含	包含
远程事务协调	包含	包含	包含	包含	包含

1.5.2 网络升级选择

如果网络已经部署了 Windows Server 2003，想升级到 Windows Server 2008 或 Windows Server 2008 R2，则有两种选择。

（1）原服务器原位升级。如果想使用原来的服务器直接升级到最新的系统，则采用这种方式。但需要注意，只能升级相同位数、相同版本。例如，如果原来安装的是 Windows Server 2003（或 Windows Server 2003 R2）的 32 位（x86）的标准版，就只能将系统升级到 Windows Server 2008 的 32 位的标准版，而不能升级到企业版或数据中心版，也不能升级到 64 位 Windows Server 2008。

（2）异构升级。如果想将当前的 32 位的 Windows Server 2003 升级到 64 位的 Windows Server 2008 或 Windows Server 2008 R2，或者想从标准版升级到企业版或数据中心版，则采用这种方式。在采用这种方式的时候，也分以下几种情况：

- 原来的服务器支持 64 位操作系统：这个时候，可以找一台“中间”服务器（称为服务器 B），在“中间”服务器上安装 Windows Server 2008 或 Windows Server 2008 R2（版本任意），升级之后，加入到域（原来的 Windows Server 2003 的 Active Directory），并且将 B 服务器升级到“主域控制器”，然后将原来的服务器（称为服务器 A）降级并从域中脱离。然后在 A 服务器上安装所需要的任何版本，再加入到 B 服务器的 Active Directory，将 A 升级到主域，B 服务器降级并从域中脱离。这样可以完成整个升级的过程。

说 明

当原来的服务器不能满足升级需求时，例如，Windows Server 2008 的升级需要系统分区（一般为 C 分区）至少 10GB 以上空间，但原来的 Windows Server 2003 的系统分区不足 10GB 时，也可以采用“中间”服务器的方式完成升级。

- 使用新的服务器，原来的服务器做额外域控制器或不再使用：只需要在新的服务器上，安装所需要的 Windows Server 2008 或 Windows Server 2008 R2，并加入到原来服务器的 Active Directory 中，将原来的服务器降级并将新的服务器升级到“主域控制器”即可。

1.6　怎样学好 Windows Server 2008 R2 系统管理

在 Windows Server 2008 R2 的学习中，涉及理论与实践两个方面的内容。理论是学习网络的基础，是指导实践的，而实践是对理论的验证。只学理论是很枯燥的，并且，如果只学理论而不加验证的话，学到的理论不容易理解，也不能真正掌握。如果只实践而不学理论的话，则实践没有了正确的方向，而且，如果在实践过程中出现问题，则不知道如何分析。所以，要学好 Windows Server 2008，理论与实践两方面都需要学习。

1.6.1　学习三步曲

那么，怎样学好 Windows Server 2008 R2 系统管理呢？推荐采用如下的步骤：

01 完全照搬阶段：在刚开始学习时，准备好实验条件，完全按照书上的要求和步骤，一步一步地做实验，达到书中实验要求的结果。

02 替换与更改阶段：在“完全按照”书上的步骤做好一个实验后，可以将实验环境还原，尝试修改实验中的“可变”数据，如 IP 地址、子网掩码、网关、DNS、计算机名称，将书中的数据换成自己设计、模拟的数据，然后使实验得到自己想要的结果。

03 排列组合阶段：书中的每个知识点（或每个功能的介绍），都可以看作一个个“单元电路”或一个个“模块”，在掌握了每个模块或单元电路，并且能“替换”其中的可变数据后，试着将已经掌握的单元电路或模块按照自己的设想进行“组合”，在这一阶段，要画网络拓扑图，标记出相应的数据、实验的目的及结果，然后自己搭建实验环境，进行实验。

04 实用阶段：在工作或者学习中有网络需求时，根据自己所掌握的单元电路，或者自己已经设计过的相同或相似电路，做出实用的网络拓扑，标记出相应的数据，在实际工作中应用。

1.6.2　掌握最基本的内容

实验是最好的老师，在理解了相关基础知识之后，就可以自己做实验。通过实验掌握所学内容，并在以后的工作中实践应用。

1.6.3　自己设计实验

设计路由器、交换机的实验涉及 TCP/IP 等知识，比较复杂，而设计网络应用类的实验所需使用的网络拓扑则比较简单了。例如，图 1-1 所示的网络拓扑图。

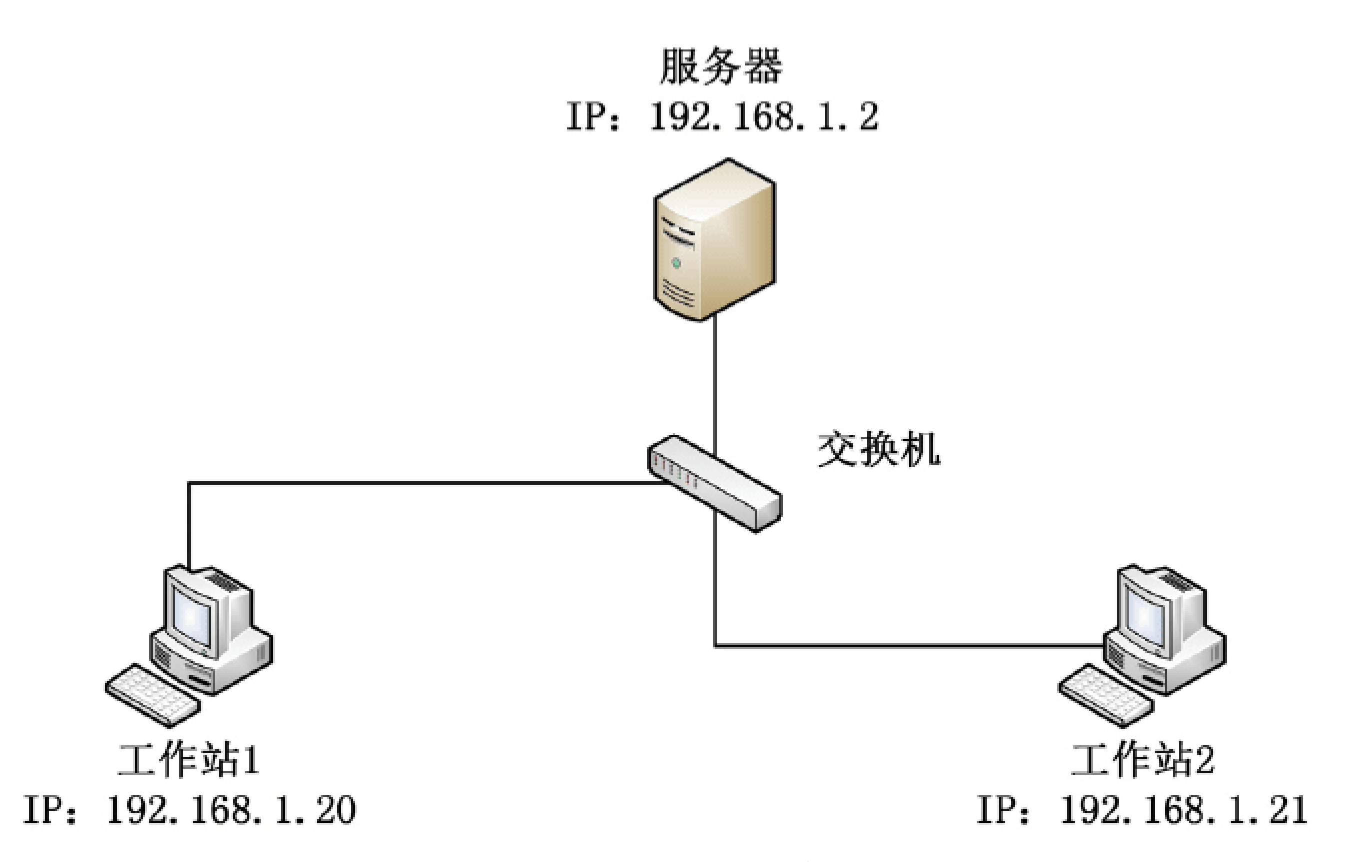


图 1-1　网络拓扑

在图 1-1 中，有 1 台服务器、2 台工作站通过 1 台交换机连接在一起。在网络应用类的实验中，主要配置“服务器”方，而工作站一端基本上很少配置，主要用来进行验证。例如，在图 1-1 中，服务器可以配置成 DHCP，工作站则通过设置为“自动获取地址”的方式验证 DHCP 服务器是否工作。

同样，利用图 1-1 的网络拓扑，还可以在服务器上安装 Windows Server 2003、Windows Server 2008，并配置成 Active Directory 服务器，而工作站可以安装 Windows XP、Windows 7 等操作系统，也加入到 Active Directory；还可以在服务器上安装 Exchange 等邮件服务器，用工作站进行验证。总之，这样的拓扑，可供实验的内容相当多。

在图 1-1 的拓扑中，当一台服务器不够用时，可以通过添加服务器，组成更加复杂的网络。如图 1-2 所示，就是一个比较“复杂”的网络拓扑。

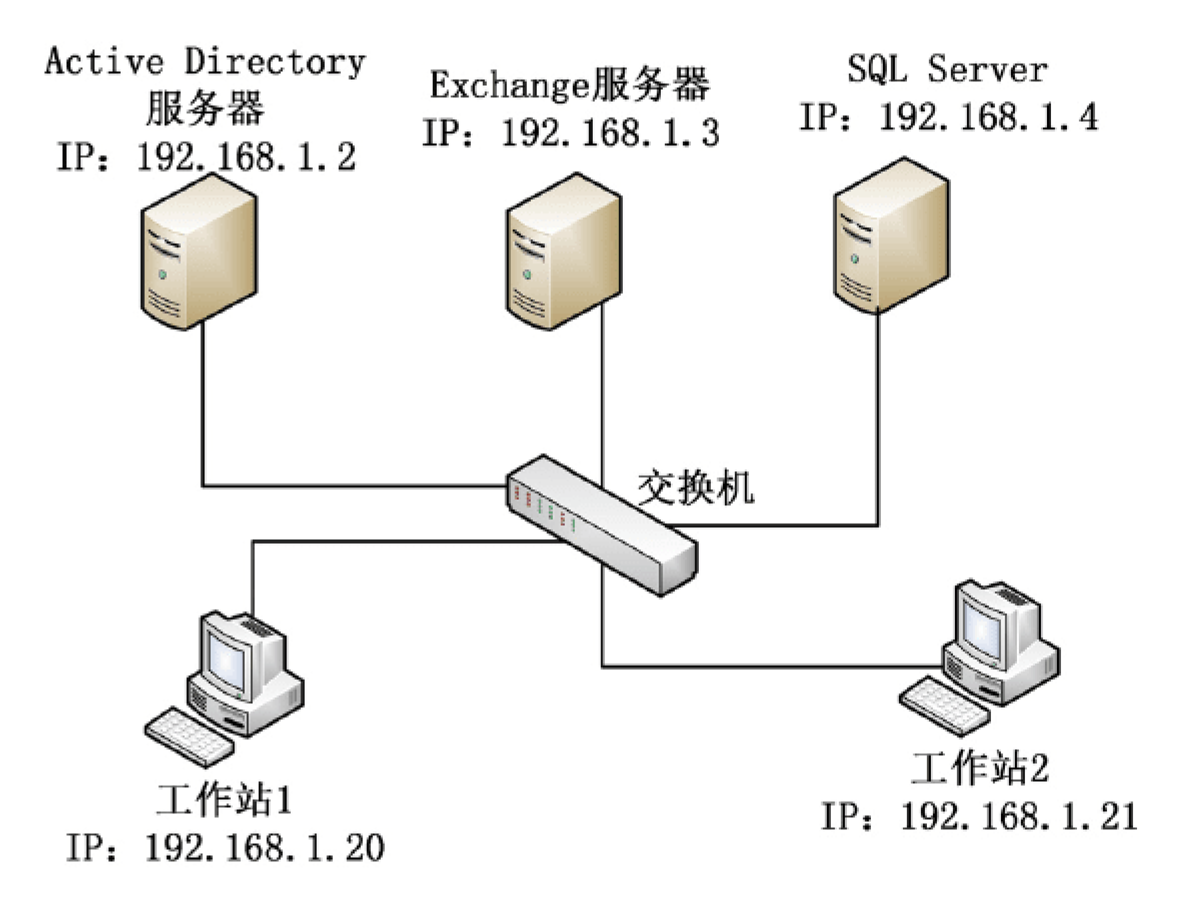


图 1-2　多台服务器网络拓扑



推 荐

可以在一台计算机上、Windows Server 2008 R2 中的 Hyper-V 虚拟机、VMware Workstation、Microsoft Virtual PC 或其他虚拟机如 Sun VirtualBox 做这些实验。

1.6.4 在实际工作中将实验进行代换

在通过实验掌握了某些内容后，在工作中，如果碰到类似的事情，可以将实验过程“拿”过来使用，但使用的时候，虽然可以“照猫画虎”，但要注意避免完全照抄。至少实验中的计算机名称、IP 地址等“可变”参数，要用实际工作中的计算机名称、IP 地址代替。另外，如果做的实验较早、内容有些陈旧，则需要重新做实验。

在“代换”的时候，要充分考虑实际的网络现状与需求。

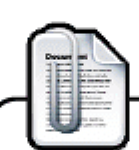
1.6.5 分析问题解决问题

网络中，不可避免会出现问题。无论是服务器端，还是客户端问题，都要在了解当前网络现状的情况下，通过分析解决问题。如果碰到以前遇到过的问题，可以凭经验解决，但有的时候，经验并不一定完全可靠。如果碰到的问题以前没有遇到过，则更要通过与用户交流、仔细分析问题并找出故障点解决。如果实在解决不了，也可以在网上搜索相关解决办法。

1.7 在 Hyper-V 虚拟机中全新安装 Windows Server 2008 R2

本节以 Windows Server 2008 R2 企业版为例，全面介绍 Windows Server 2008 R2 的安装。由于 Windows Server 2008 R2 是 Windows Server 2008 的升级版，在本书中，如无特殊说明，所介绍的内容与操作也适用于 Windows Server 2008，在介绍到 Windows Server 2008 R2 的“专有内容”时，会特别说明。

本书不过多介绍理论内容，以实践、实战为主。每一章会介绍几个知识点，并通过案例的方式展现。为了保持实验的一致性，我们将在 Windows Server 2008 R2 的 Hyper-V 虚拟机中，安装配置这些内容。



说 明

本章将只介绍 Windows Server 2008 R2 的安装，有关 Windows Server 2008 R2 中 Hyper-V 的配置与使用，可参见本书第 11 章的内容。

1.7.1 在 Hyper-V 虚拟机中安装 Windows Server 2008 R2

在 Hyper-V 中创建 Windows Server 2008 R2 的虚拟机，并在虚拟机中安装 Windows Server 2008 R2，主要步骤如下：

01 在“Hyper-V 管理控制台”中，创建名为 ws08r2 的虚拟机（如图 1-3 所示），并设置虚拟机内存为 1GB（如图 1-4 所示）、使用 Windows Server 2008 R2 光盘镜像作为虚拟机的光驱（如图 1-5 所示）。



图 1-3　设置虚拟机的名称

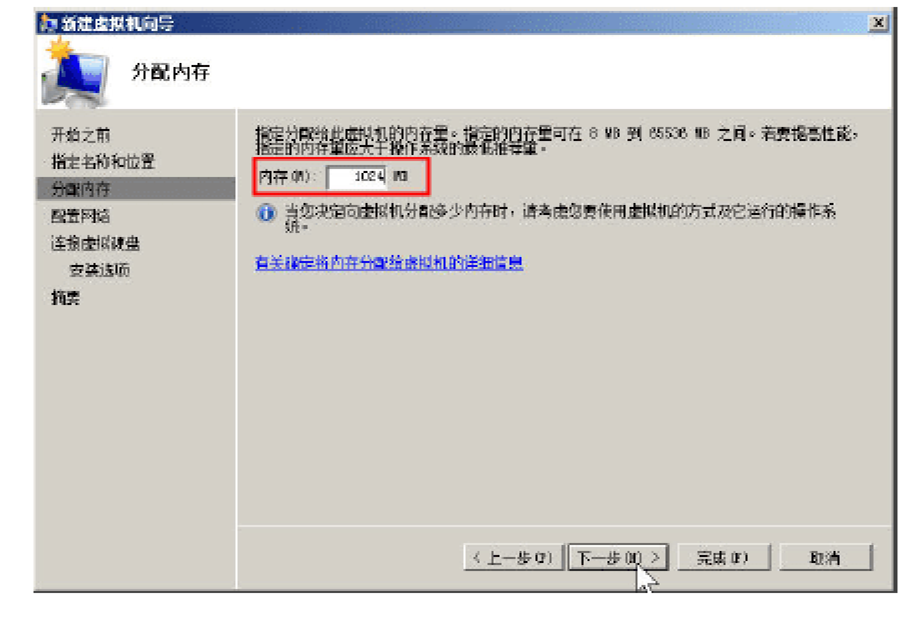


图 1-4　为虚拟机分配 1GB 内存

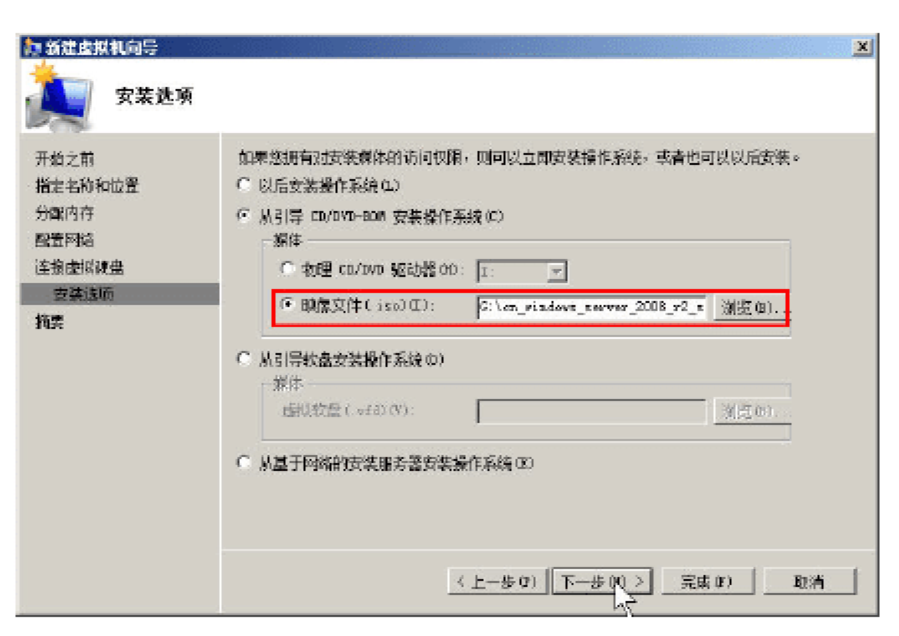


图 1-5　使用 Windows Server 2008 R2 光盘镜像作为虚拟机的光驱

02 在创建虚拟机完成之后，启动该虚拟机。

03 启动虚拟机之后，进入安装语言、时间和货币格式选择，在此选择“中文（简体）”，然后单击“下一步”按钮，如图 1-6 所示。

04 在“现在安装”对话框中，单击“现在安装”按钮，如图 1-7 所示。

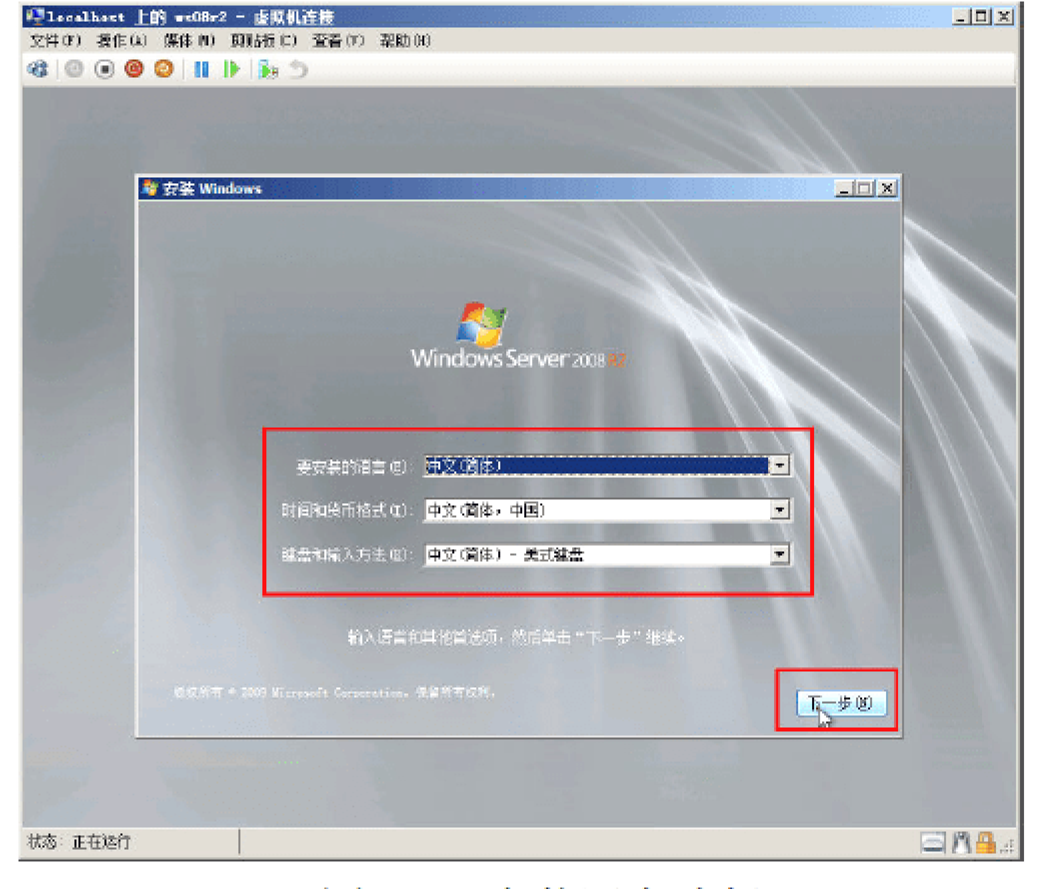


图 1-6　安装语言选择

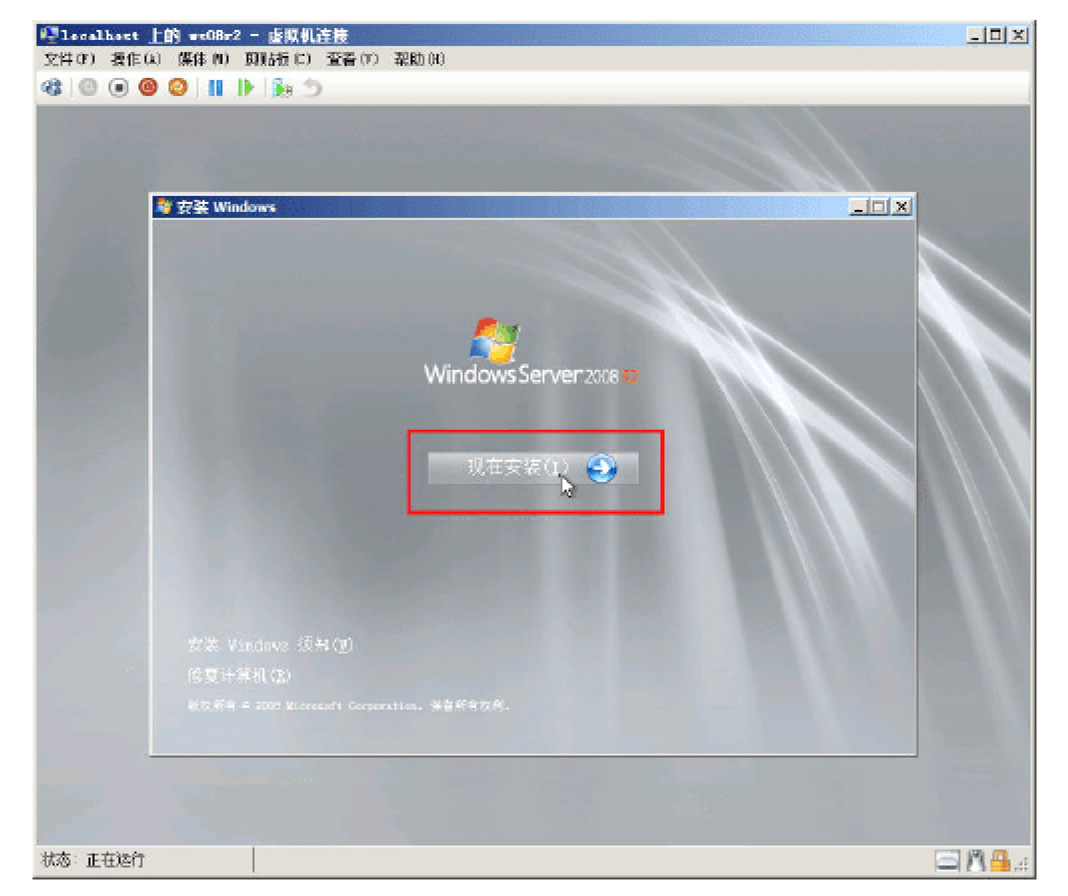


图 1-7　现在安装

05 在“选择要安装的操作系统”对话框中，选择“Windows Server 2008 R2 Enterprise（完全安装）”选项，然后单击“下一步”按钮，如图 1-8 所示。

06 在“请阅读许可条款”对话框中，选中“我接受许可条款”复选框，然后单击“下一步”按钮，如图 1-9 所示。

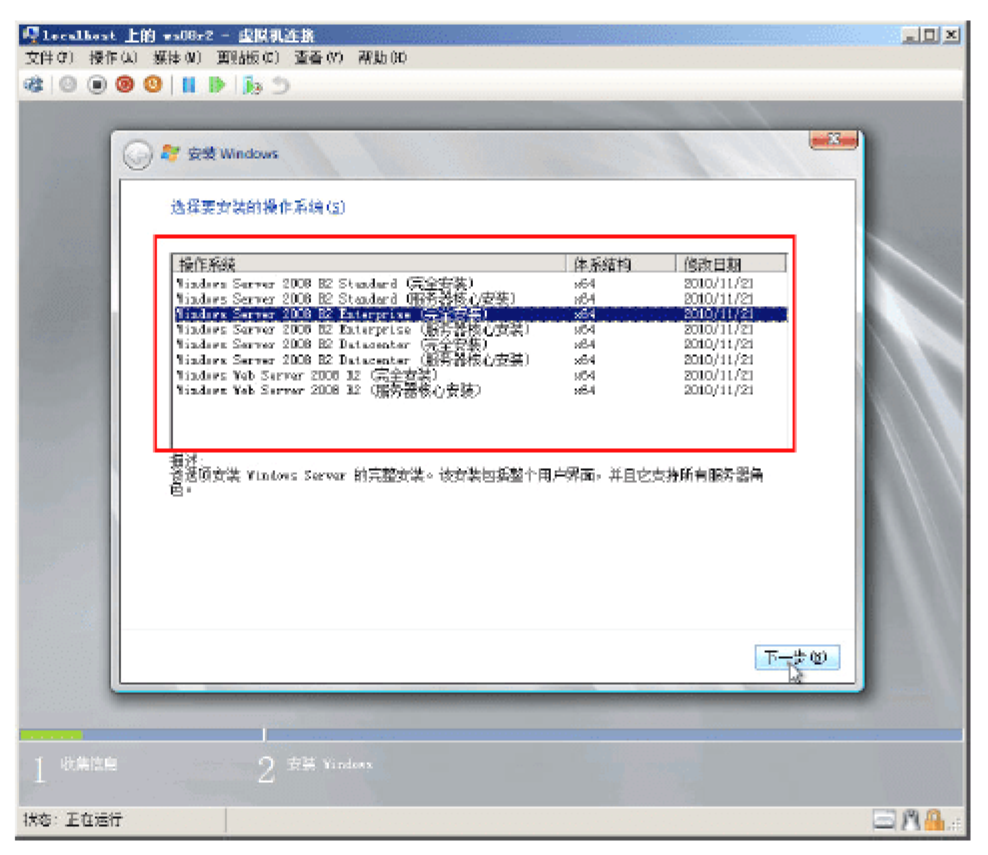


图 1-8　选择要安装的操作系统

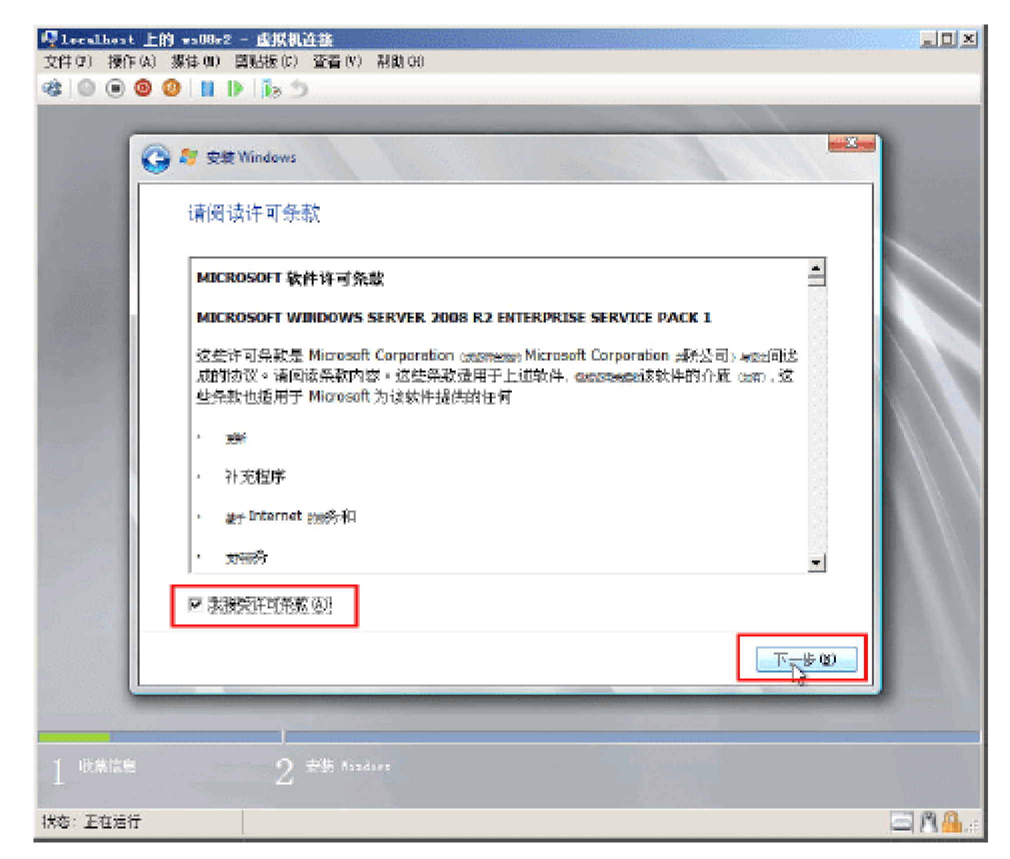


图 1-9　接受许可条款

07 在“您想进行何种类型的安装”对话框中，单击“自定义（高级）”图标，如图 1-10 所示。

08 在“您想将 Windows 安装在何处”对话框中，选择当前计算机（虚拟机）中的硬盘，单击“下一步”按钮，如图 1-11 所示。

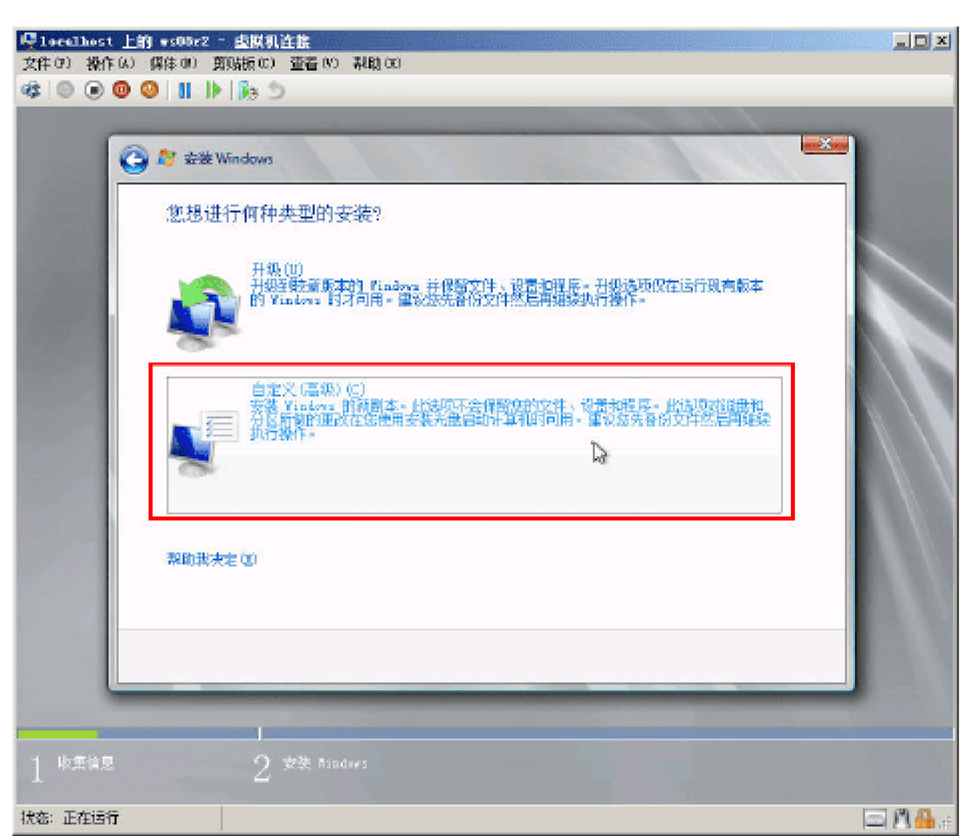


图 1-10　自定义安装

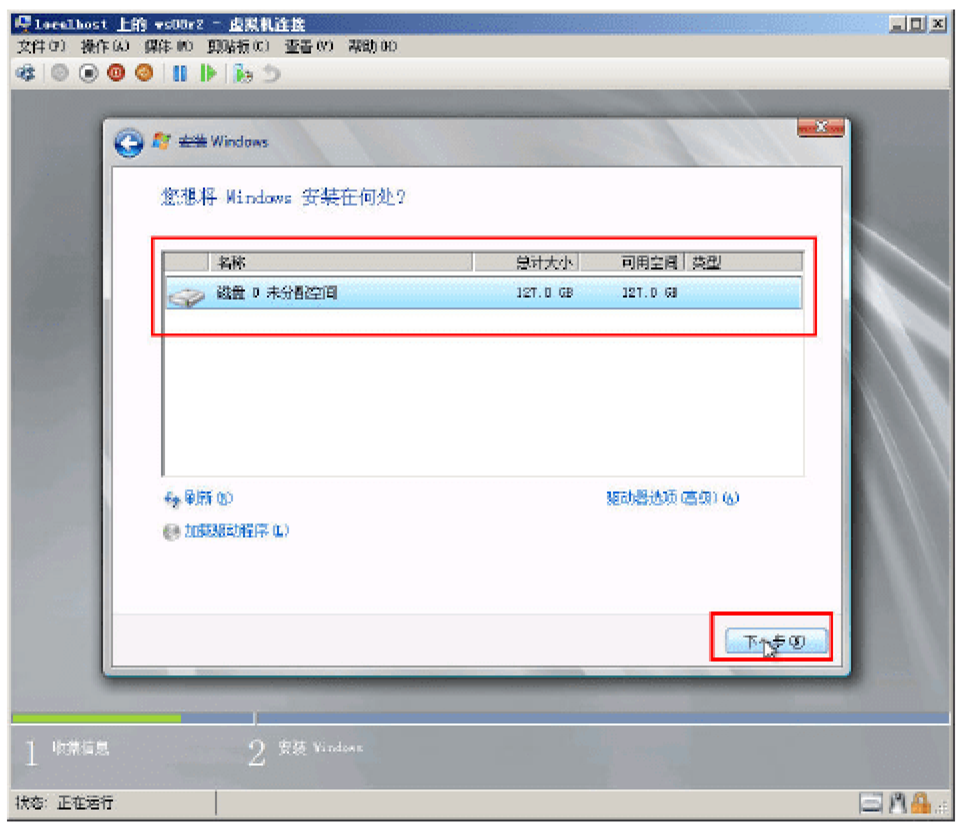


图 1-11　选择安装磁盘

说 明

从光盘启动，只能选择“自定义”安装，如果当前计算机的硬盘有 Windows Server 2003 等操作系统，想进行升级安装，可进入 Windows Server 2003 操作系统，运行 Windows Server 2008 R2 安装程序。

（1）虽然 Windows Server 2008 R2 已经集成了当前许多主流计算机及服务器的 SCSI、RAID 卡、SAS 卡的驱动程序，但硬件的发展日新月异，如果你的计算机或服务器的硬盘接口（主要是一些新的 SAS RAID 卡）不支持 Windows Server 2008（或 Windows Server 2008 R2），请单击“加载驱动程序”，并插入硬件厂商提供的驱动程序光盘，加载并安装 Windows Server 2008 的驱动程序，然后再安装系统。（2）在真正的主机或服务器中，安装时，如果是新的硬盘，可以单击“驱动器选项（高级）”，对当前硬盘进行分区，但不推荐这样做。即使是服务器的硬盘，你也可以在安装完操作系统之后，使用 Windows Server 2008 提供的硬盘管理工具，调整当前分区的大小，并创建新的分区。

09 之后，安装程序开始 Windows Server 2008 R2 的安装，如图 1-12 所示。这个安装过程大约需要 30 分钟的时间，在这个安装的过程中，用户可以返回到主机，进行其他操作。

10 安装完 Windows Server 2008 R2 之后，在第一次登录的时候，需要修改密码，如图 1-13 所示。

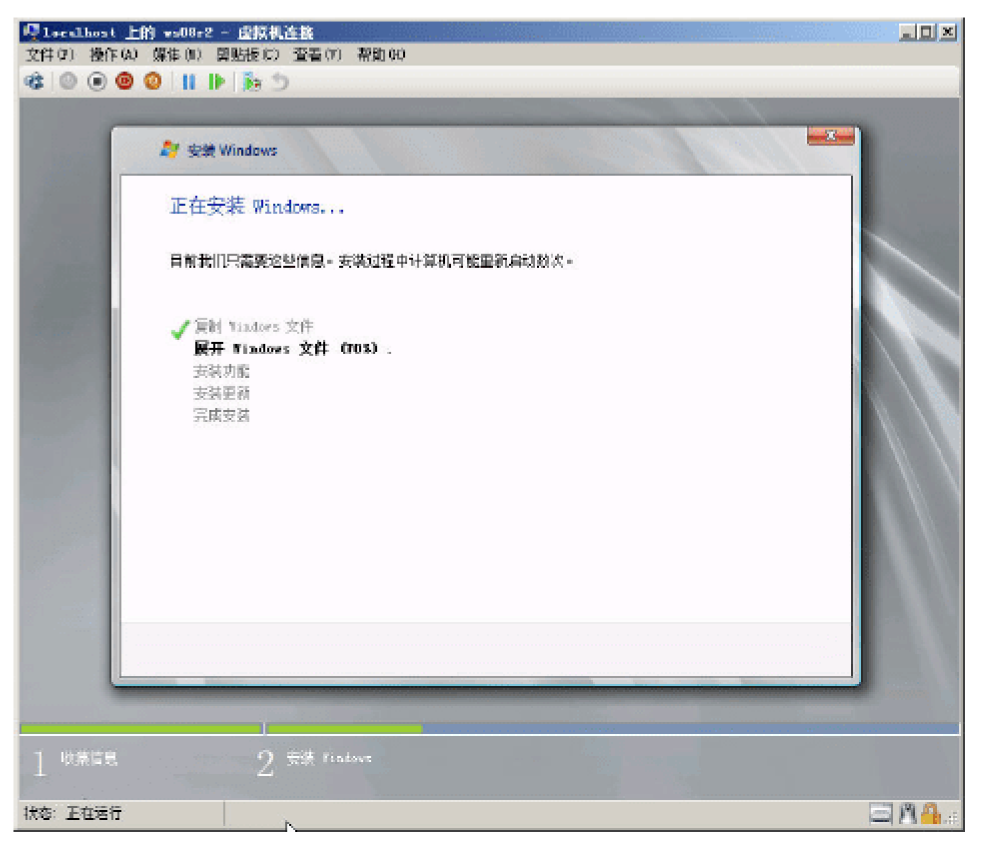
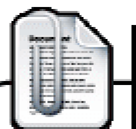


图 1-12 Windows Server 2008 的安装界面



图 1-13 首次登录更改密码



说 明

在没有安装 Hyper-V 的“集成服务安装盘—虚拟机的驱动程序”之前，鼠标不能直接从虚拟机中“移动”到“主机”中，如果你想从虚拟机的控制中返回到主机，请按热键“Ctrl+Alt+←（即左箭头键）”，这样就可以返回到主机控制状态了。以后想控制虚拟机，用鼠标在虚拟机的窗口中单击一下就可以。

11 在设置密码时，需要设置复杂密码，即包括大写字母、“！·#￥%”、数字、小写字母四类中的 3 种，并且长度超过 6 位，在本例中，设置密码为 a1b2c3D4，其中 D 是大写字母，如图 1-14 所示。

12 在“初始配置任务”窗口中，选中“登录时不显示此窗口”复选框，然后单击“关闭”按钮，如图 1-15 所示。

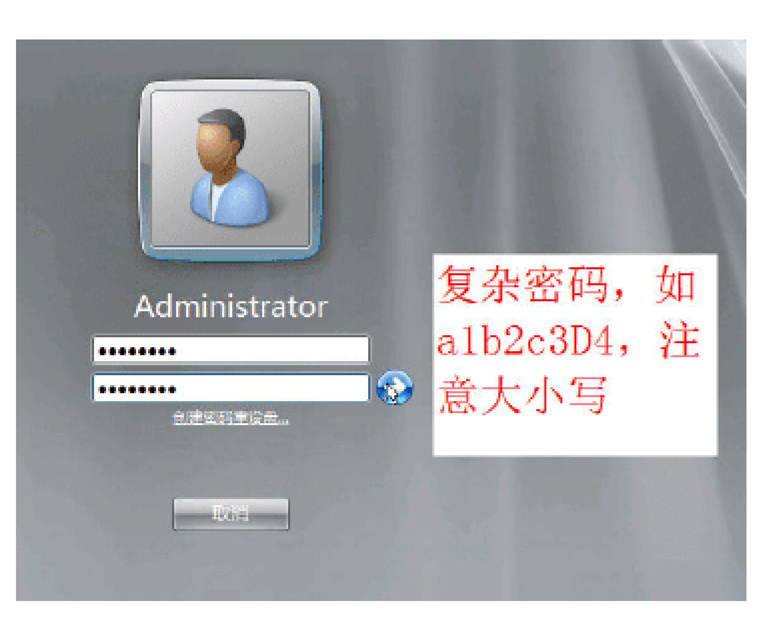


图 1-14 设置复杂密码

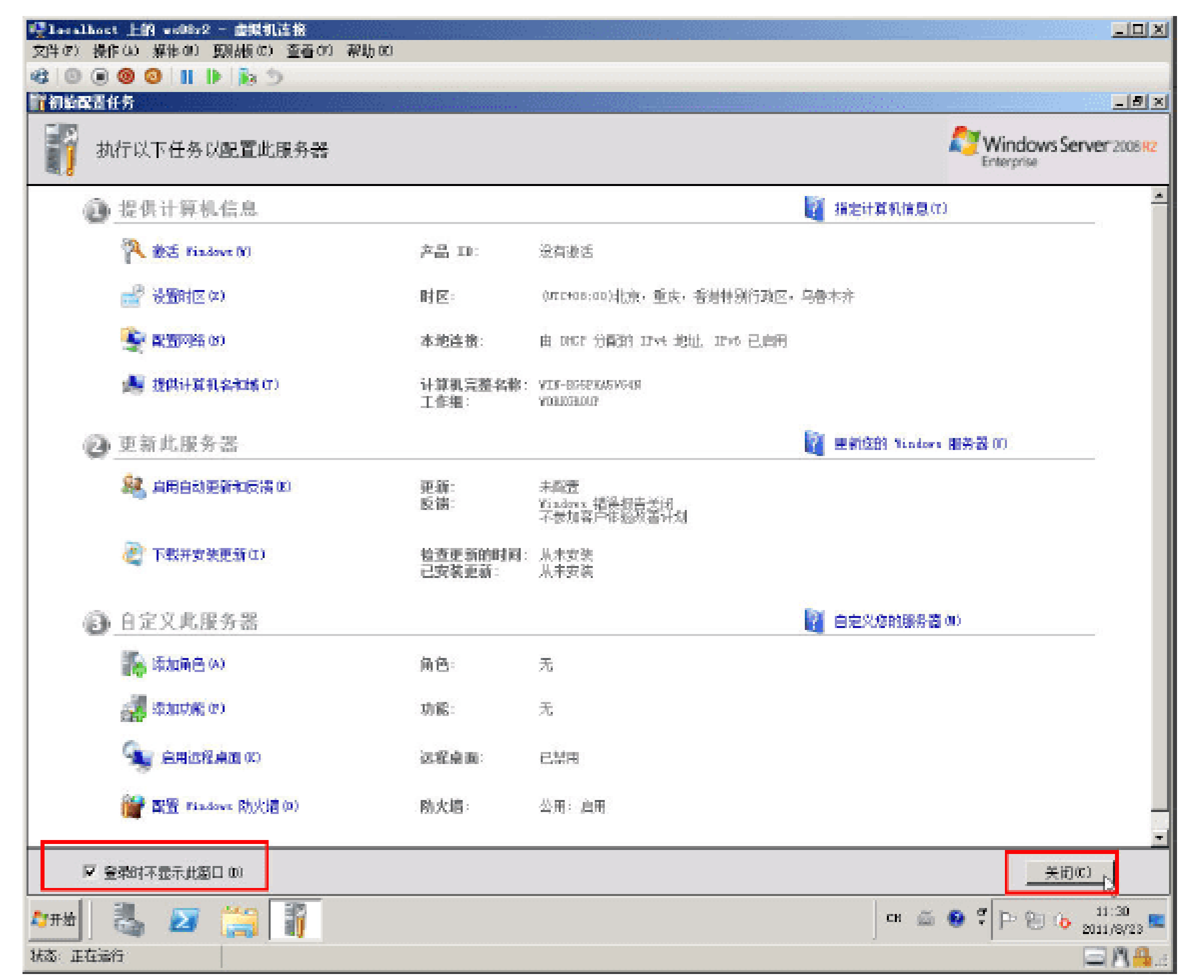


图 1-15 关闭初始配置任务

1.7.2 安装虚拟机驱动程序

在安装完 Windows Server 2008 R2 之后，为了提高虚拟机的性能，还要安装称为“集成服务安装盘”的虚拟机驱动程序，主要步骤如下：

01 按“Ctrl+Alt+←”按键切换到主机，在“操作”菜单中选择“插入集成服务安装盘”菜单项，如图 1-16 所示。

02 进入虚拟机之后，在弹出的“自动播放”对话框中，单击“安装 Hyper-V 集成服务”链接，开始运行虚拟机附加程序，如图 1-17 所示。

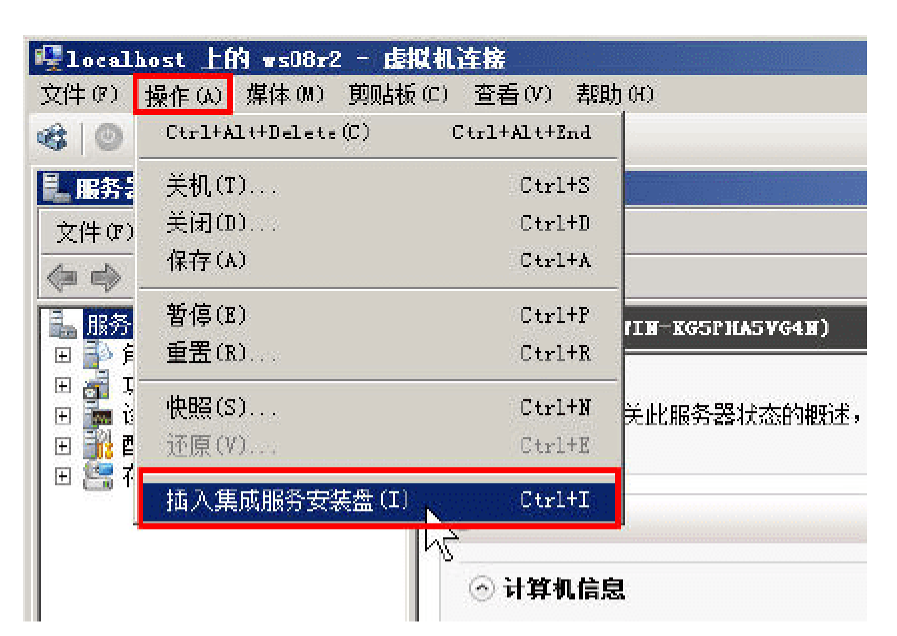


图 1-16 安装虚拟机附加程序

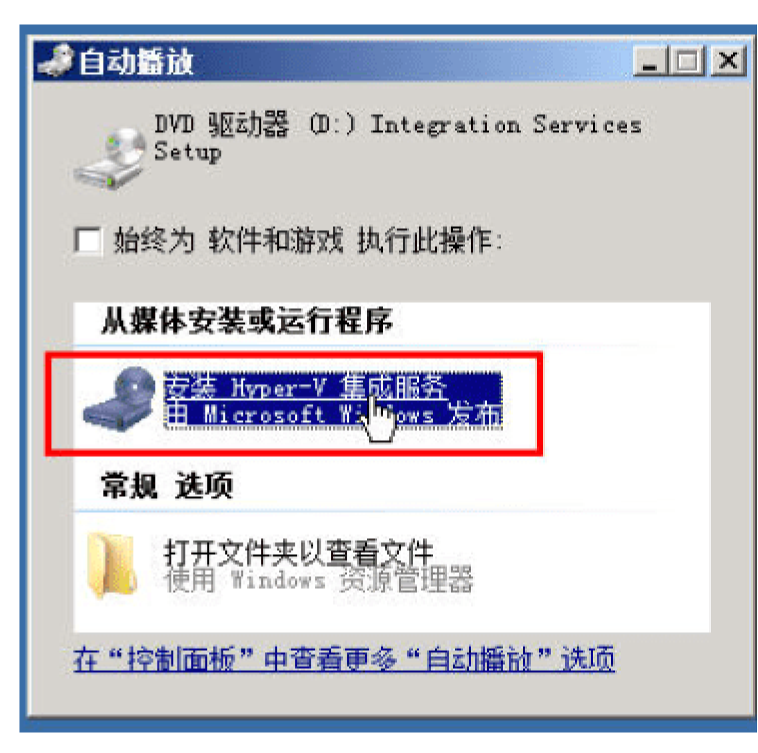


图 1-17 安装集成服务

03 在“升级 Hyper-V 集成服务”对话框中，单击“确定”按钮，如图 1-18 所示。

04 在随后的过程中，Hyper-V 集成服务开始安装 Windows 驱动程序，如图 1-19 所示。

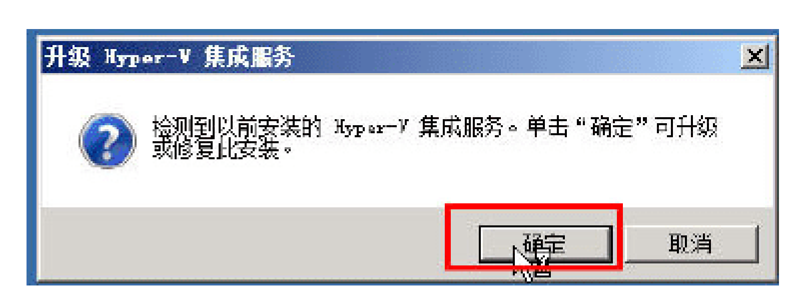


图 1-18 升级

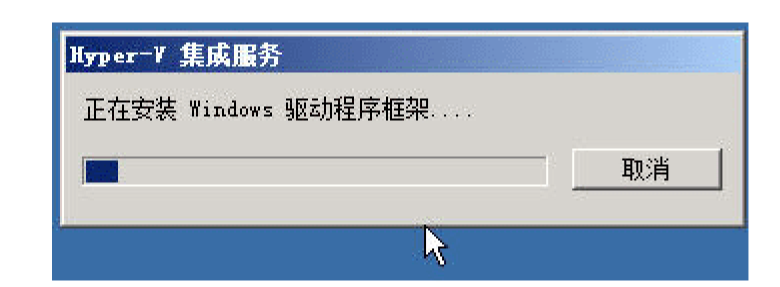


图 1-19 开始安装

05 安装程序完成之后，单击“是”按钮，如图 1-20 所示，重新启动虚拟机。

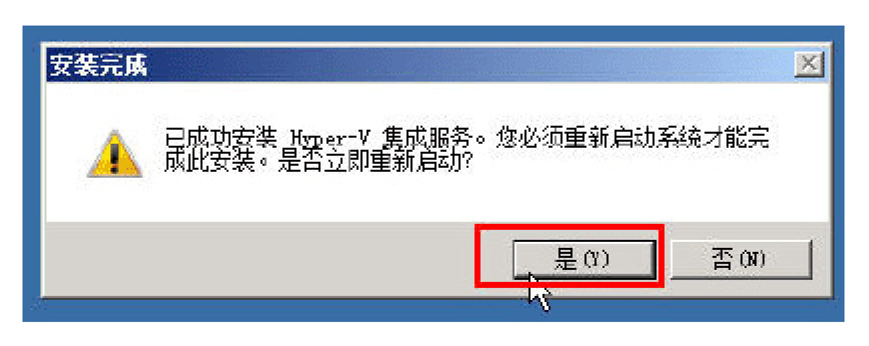


图 1-20 安装完成

当再次进入系统后，鼠标就可以直接在“虚拟机”与“主机”之间自由切换了，并且虚拟机的性能会有所提高。

1.7.3 Windows Server 2008 R2 的基本配置

在安装完虚拟机的驱动程序之后，再次进入 Windows Server 2008 R2。下面介绍 Windows Server 2008 R2 的基本配置。

1. 登录进入系统

首先，按下“Ctrl+Alt+End”按键，或者在“操作”菜单中选择“Ctrl+Alt+Delete”命令，开始登录，如图 1-21 所示。然后输入用户名、密码，登录进入系统。

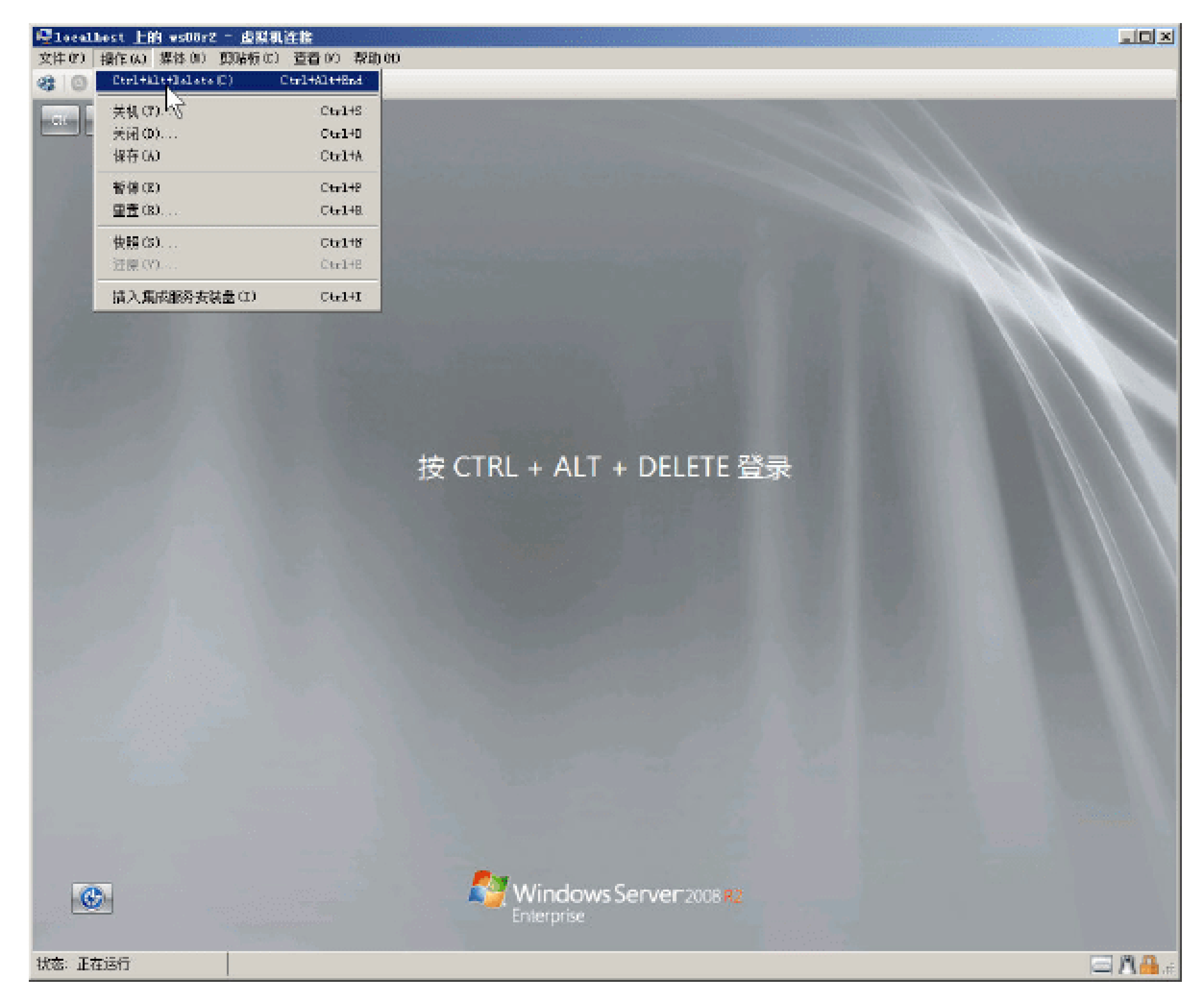


图 1-21　开始登录

2. 关闭屏幕保护程序

对于虚拟机来说（包括 Hyper-V Server 的虚拟机、VMware 的虚拟机），建议关闭“屏幕保护程序”，以提高虚拟机的性能。

01 打开“控制面板→所有控制面板选项→显示”窗口，单击“更改屏幕保护程序”链接，如图 1-22 所示。

02 在弹出的“屏幕保护程序设置”对话框中，在“屏幕保护程序”下拉列表中选择“无”，如图 1-23 所示。

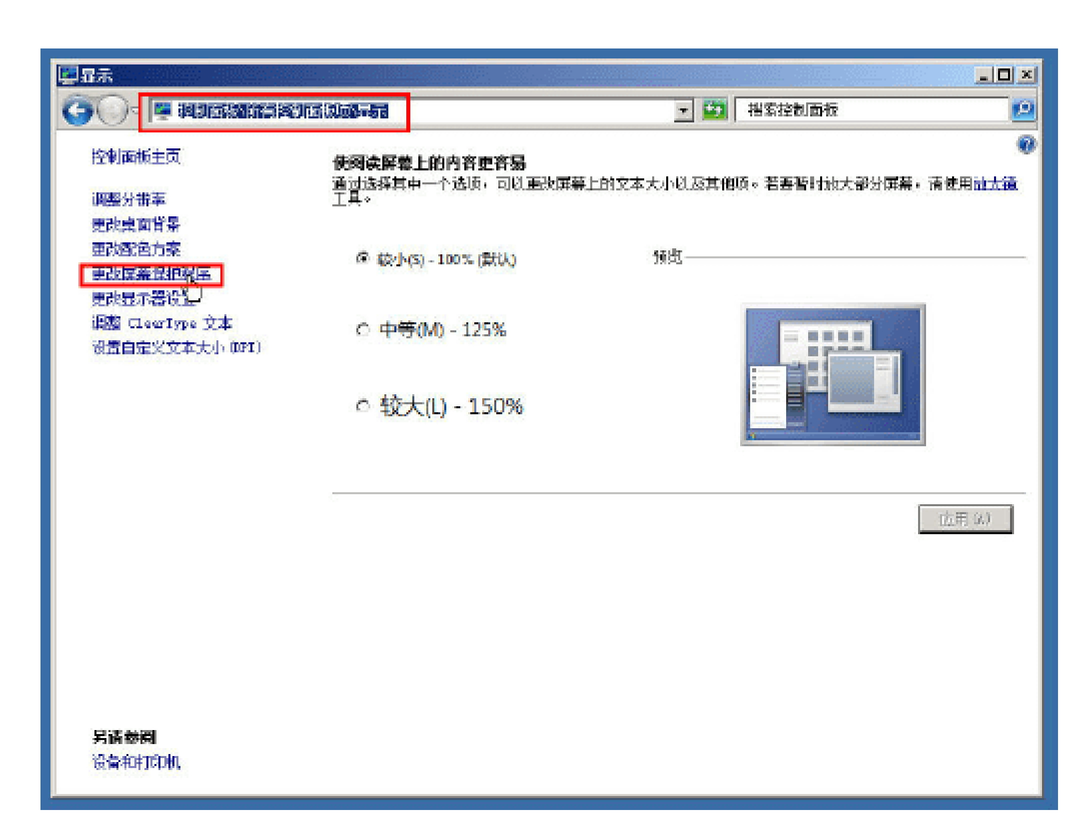


图 1-22　显示选项

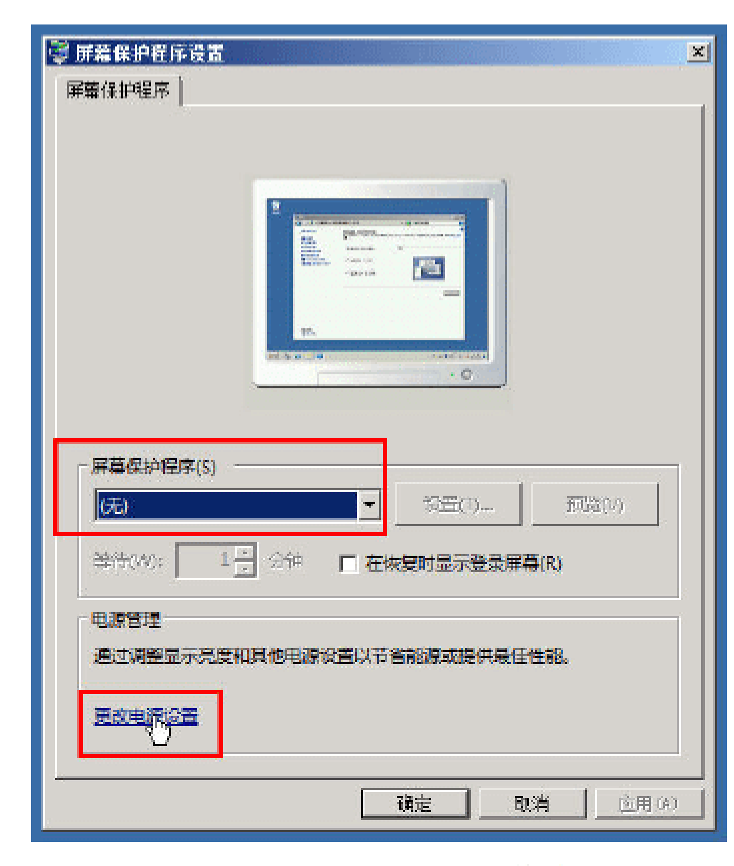


图 1-23　取消屏幕保护

03 然后单击“更改电源设置”按钮，在弹出的“电源选项”对话框中，在“平衡”处单击

“更改设计设置”链接；在弹出的“更改计划的设置：平衡”对话框中，在“关闭显示器”下拉列表中选择“从不”，如图 1-24 所示。然后单击“保存修改”按钮返回“电源选项”，并关闭这个对话框返回到“屏幕保护程序设置”对话框，单击“确定”按钮。

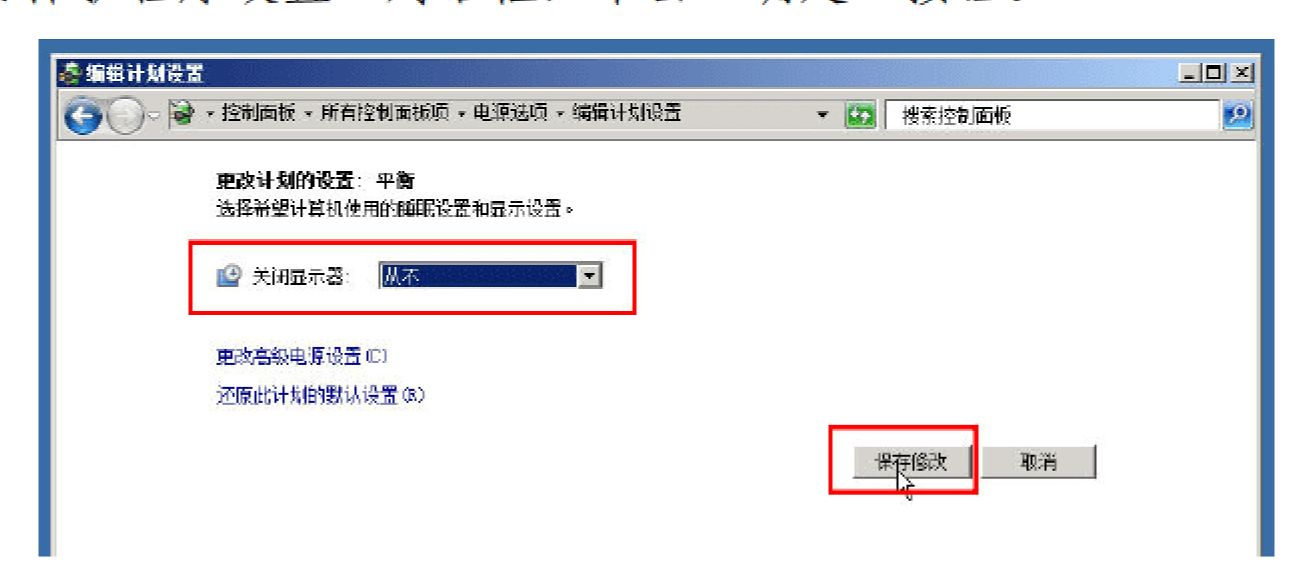


图 1-24 从不关闭显示器

3. 压缩卷并创建新的分区

在前面安装系统的时候，我们介绍过，选择整个硬盘安装系统，并在安装系统完成之后，使用 Windows Server 2008 R2 自带的磁盘管理工具调整分区的大小，并创建新的分区。接下来我们介绍操作步骤。

01 进入“服务器管理器”窗口，在左侧窗格中定位到“存储→磁盘管理”选项，在右侧的“磁盘管理”列表中，选中要进行压缩的磁盘，单击鼠标右键，在弹出的快捷菜单中选择“压缩卷”命令，如图 1-25 所示。

02 在弹出的“压缩 C: ”对话框中，显示了“压缩前的总计大小”、“可用压缩空间大小”，在“输入压缩空间量”文本框中输入 61085MB，然后单击“压缩”按钮，如图 1-26 所示。

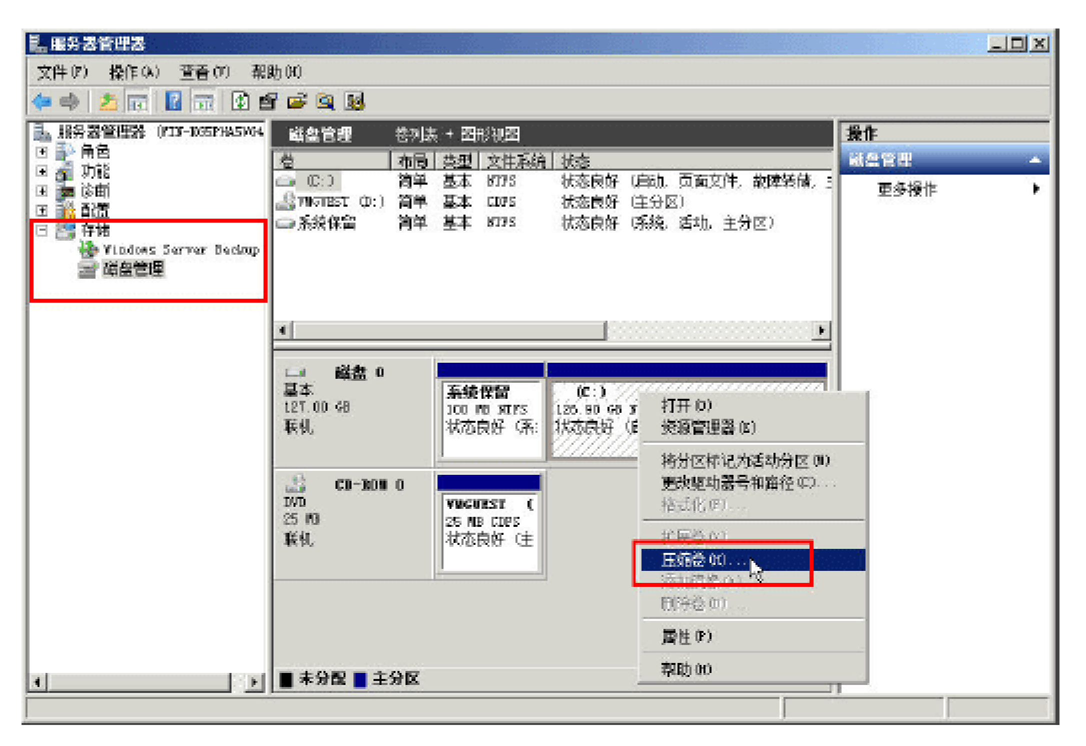


图 1-25 压缩卷

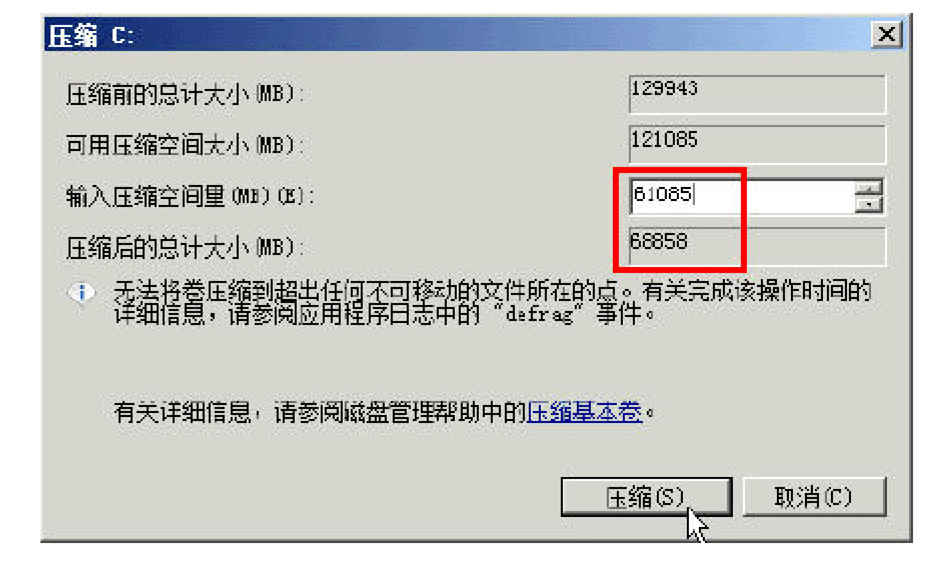
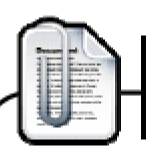


图 1-26 压缩



说 明

对于 Windows Server 2008，建议 C 盘最小空间为 40GB；对于 Windows Server 2008 R2 来说，建议 C 盘最小为 50～60GB。这样以后无论升级到更新的版本，还是打补丁、安装驱动等，或是安装一些必须的系统文件，都会有足够的空间。当然，即使磁盘空间不够，也可以使用“扩展卷”的方式，调整分区的大小，这些内容会在后面的章节介绍。

03 压缩之后，当前磁盘的右侧会有压缩后的大小（压缩节省下来的空间），用鼠标右击，在弹出的快捷菜单中选择“新建简单卷”命令，如图 1-27 所示。

04 在“新建简单卷向导”对话框中，单击“下一步”按钮，进入“指定卷大小”对话框，单击“下一步”按钮，使用最大的可用空间。在“分配驱动器号和路径”对话框中，为新建卷分配驱动器号，如图 1-28 所示。

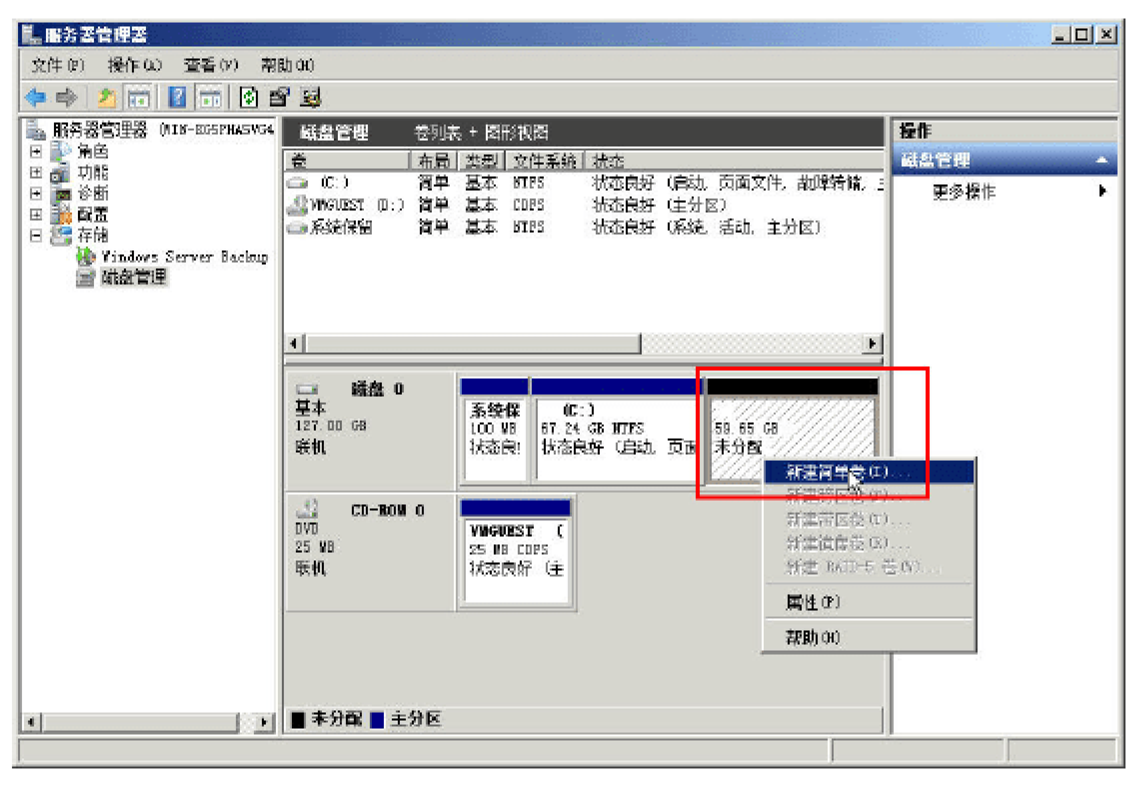


图 1-27　新建简单卷

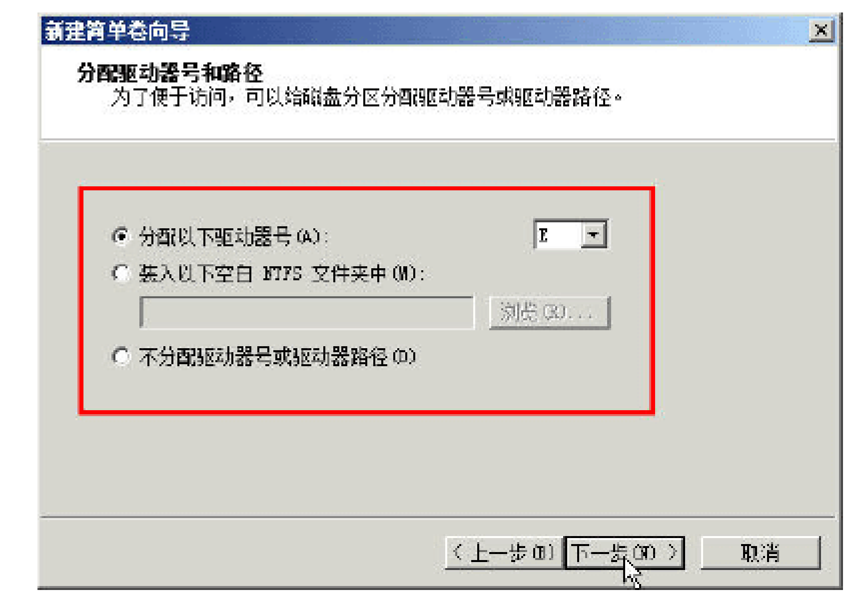
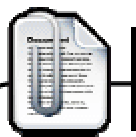


图 1-28　分配驱动器号和路径



说 明

用户可以在“分配以下驱动器号”下拉列表中，为新建的卷选择其他不同的盘符；也可以选择“装入以下空白 NTFS 文件夹中”，在现有的盘符中，创建一个新的文件夹，将新建的卷装入到这个文件夹中；也可以选择“不分配驱动器号或驱动器路径”，以后再进行分配。

05 在“格式化分区”对话框中，用 NTFS 文件系统，格式化新建卷，并为新建分区创建卷标，如图 1-29 所示。

06 在“正在完成新建简单卷向导”对话框，单击“完成”按钮，创建卷完成。这样，在不损坏现有分区、不丢失数据的前提下，我们使用 Windows Server 2008 R2 的“磁盘管理”工具，在只有一个分区的情况下，创建并添加了一个新的分区。添加后的界面如图 1-30 所示。

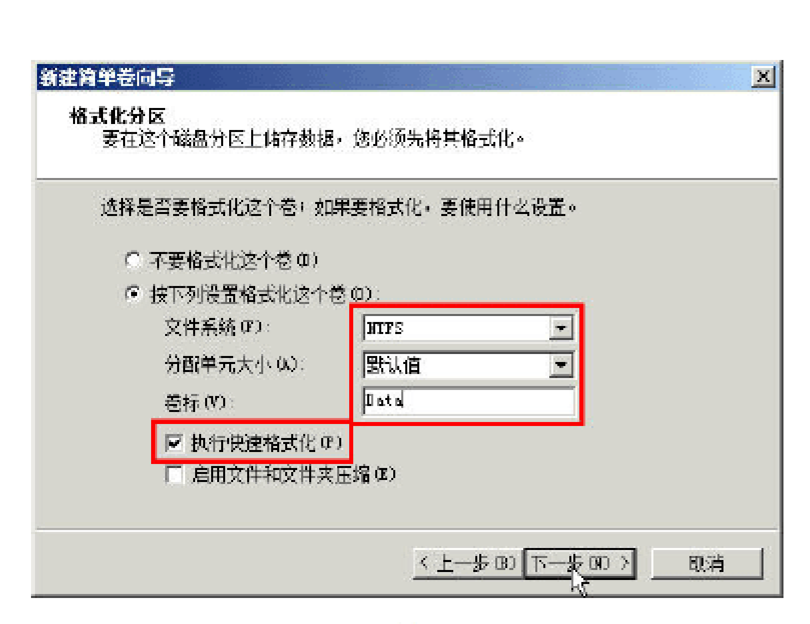


图 1-29　格式化分区

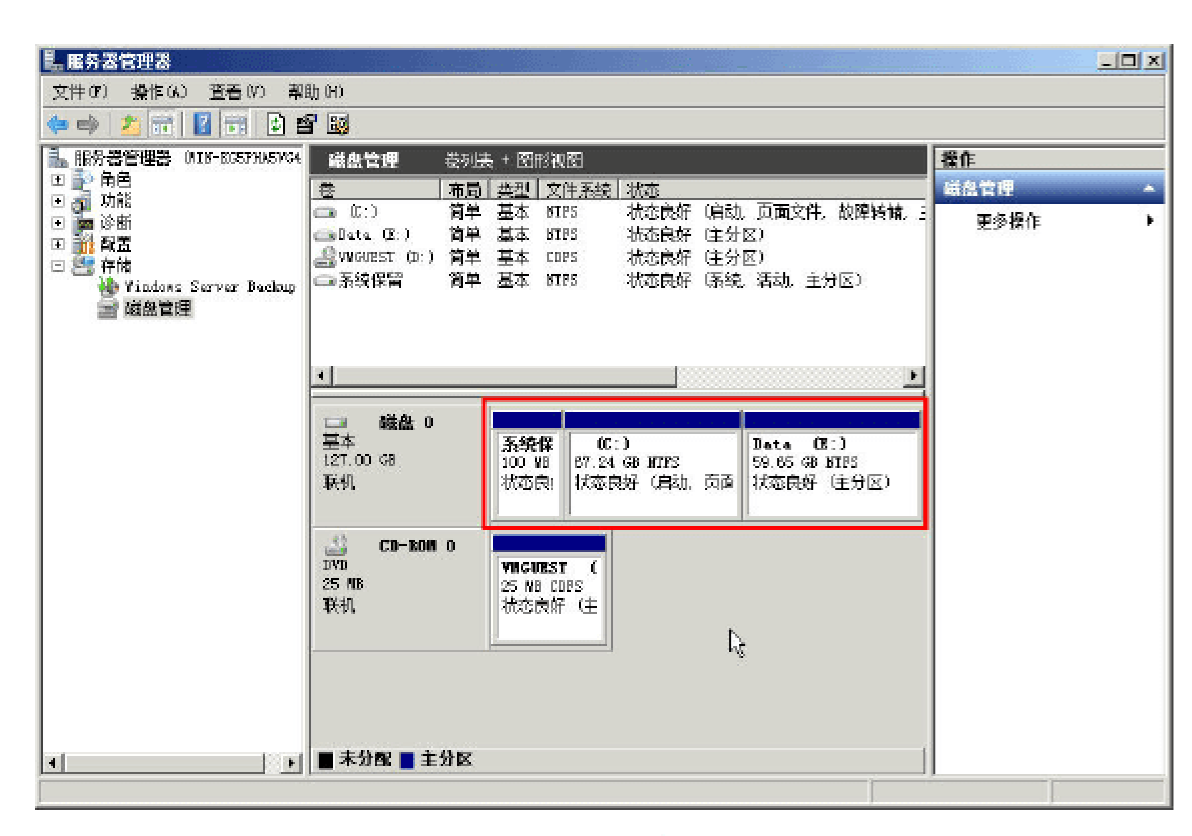


图 1-30　创建并添加新分区



说 明

Windows Vista 及其以后的操作系统，所包括的“磁盘管理”功能，都可以调整分区、压缩卷、管理卷功能，我们将在以后的章节中，详细介绍这个功能。

4. 修改本地策略

从 Windows NT 操作系统开始，每次登录界面都会要求用户按下“Ctrl+Alt+Del”键，如果你想取消这个功能，可以通过修改“本地组策略”来实现。

01 运行 gpedit.msc，如图 1-31 所示。

02 在打开的“本地组策略编辑器”对话框中，在左侧的窗格中定位到“计算机配置→Windows 设置→安全设置→本地策略→安全选项”，双击右侧的“交互式登录：无须按 Ctrl+Alt+Del”命令，在弹出的“交互式登录：无须按 Ctrl+Alt+Del 属性”对话框中，选中“已启用”单选按钮，如图 1-32 所示。

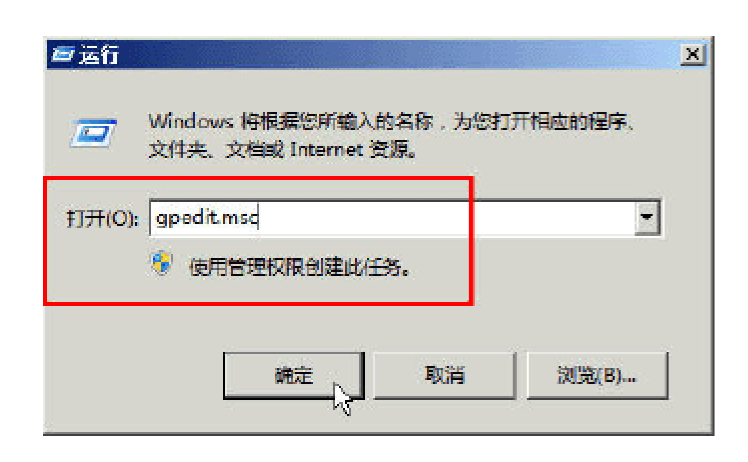


图 1-31　运行 gpedit.msc

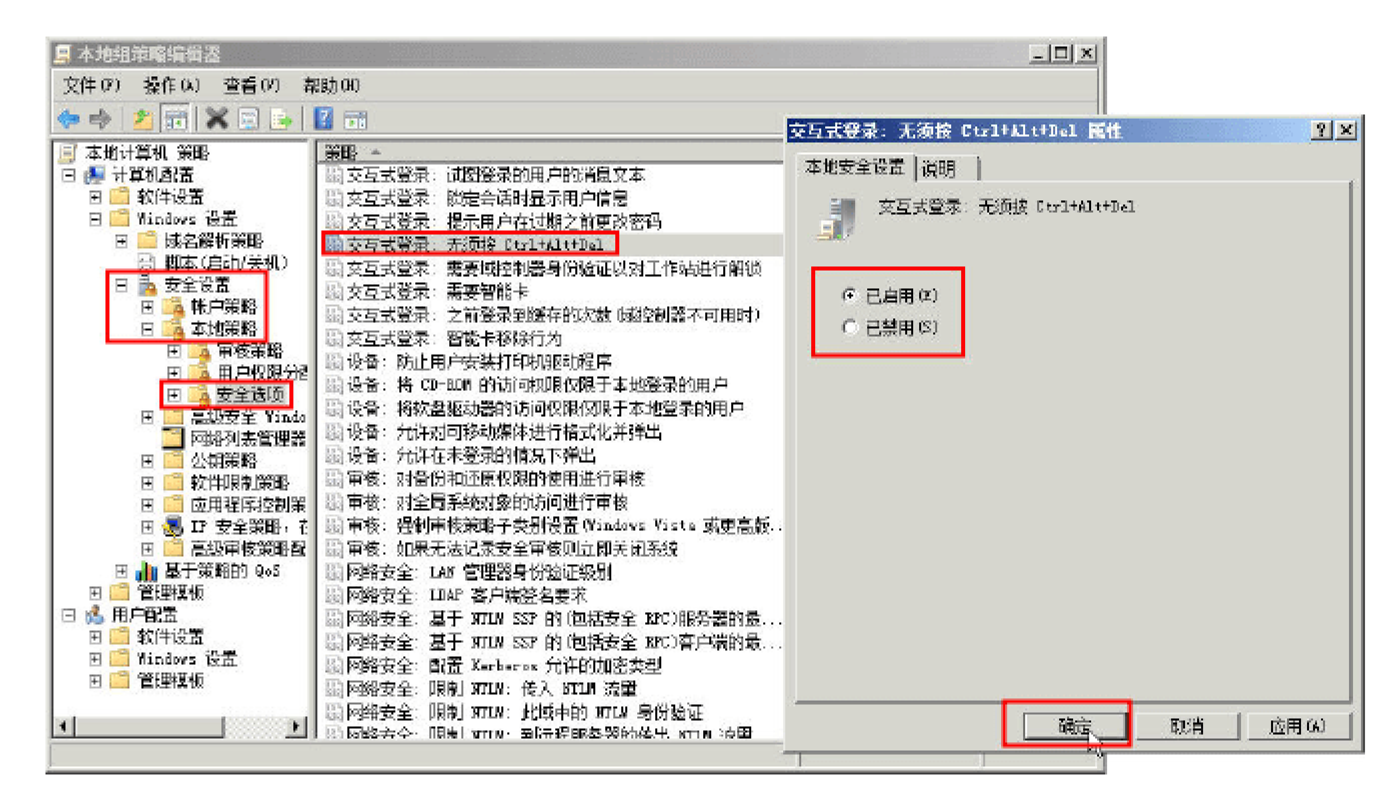


图 1-32　取消登录前 Ctrl+Alt+Del 的设置

03 在左侧的窗格中定位到“管理模板→系统”，修改“激活‘关闭事件跟踪程序系统状态数据’功能”为“已禁用”，修改“显示‘关闭事件跟踪程序’”为“已禁用”，修改“在登录时不显示‘管理您的服务器’页”为“已启用”，如图 1-33 所示。然后关闭本地策略编辑器。

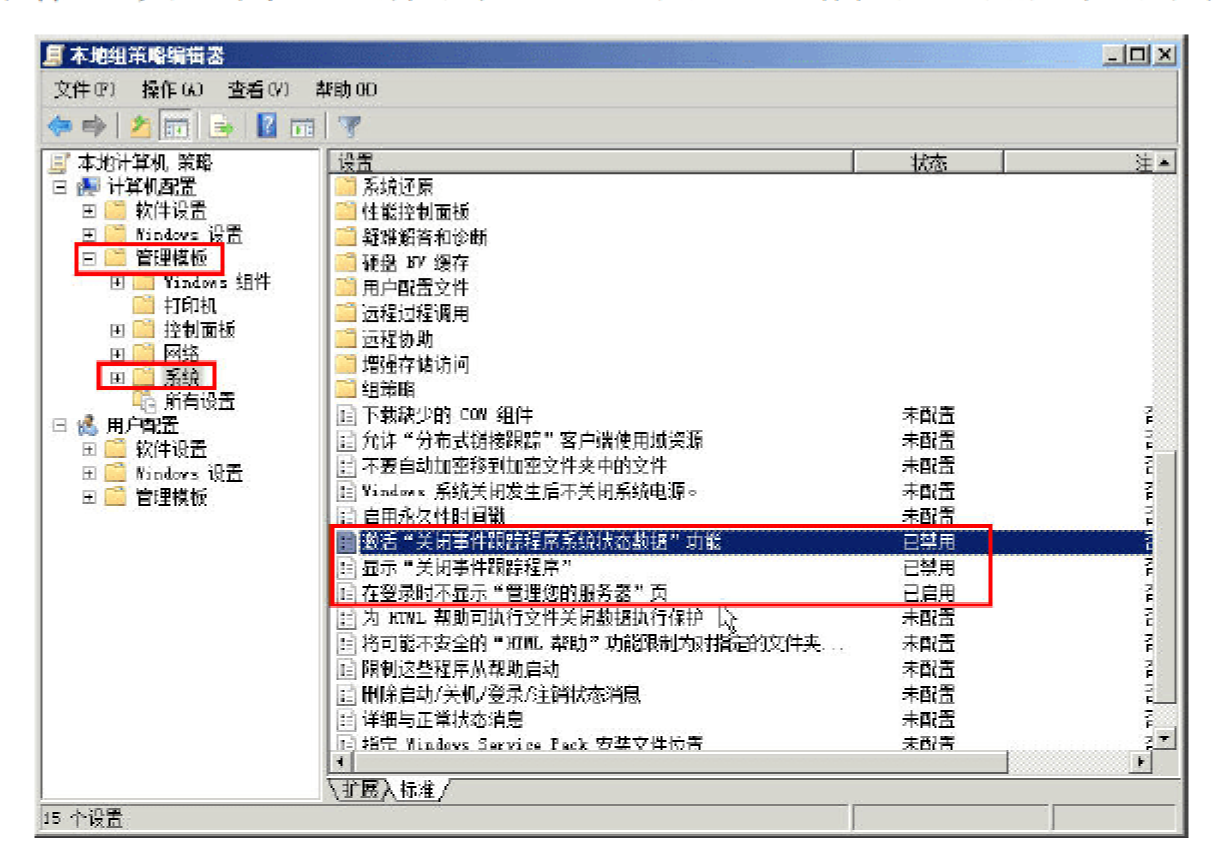


图 1-33　修改系统策略

04 打开“服务器管理器”窗口，在“安全信息”选项组中单击“配置 IE SEC”链接，在弹出的“Internet　Explorer 增强的安全配置”对话框中，在“管理员”和“用户”字段中均选中“禁用”单选按钮，然后单击“确定”按钮，如图 1-34 所示。

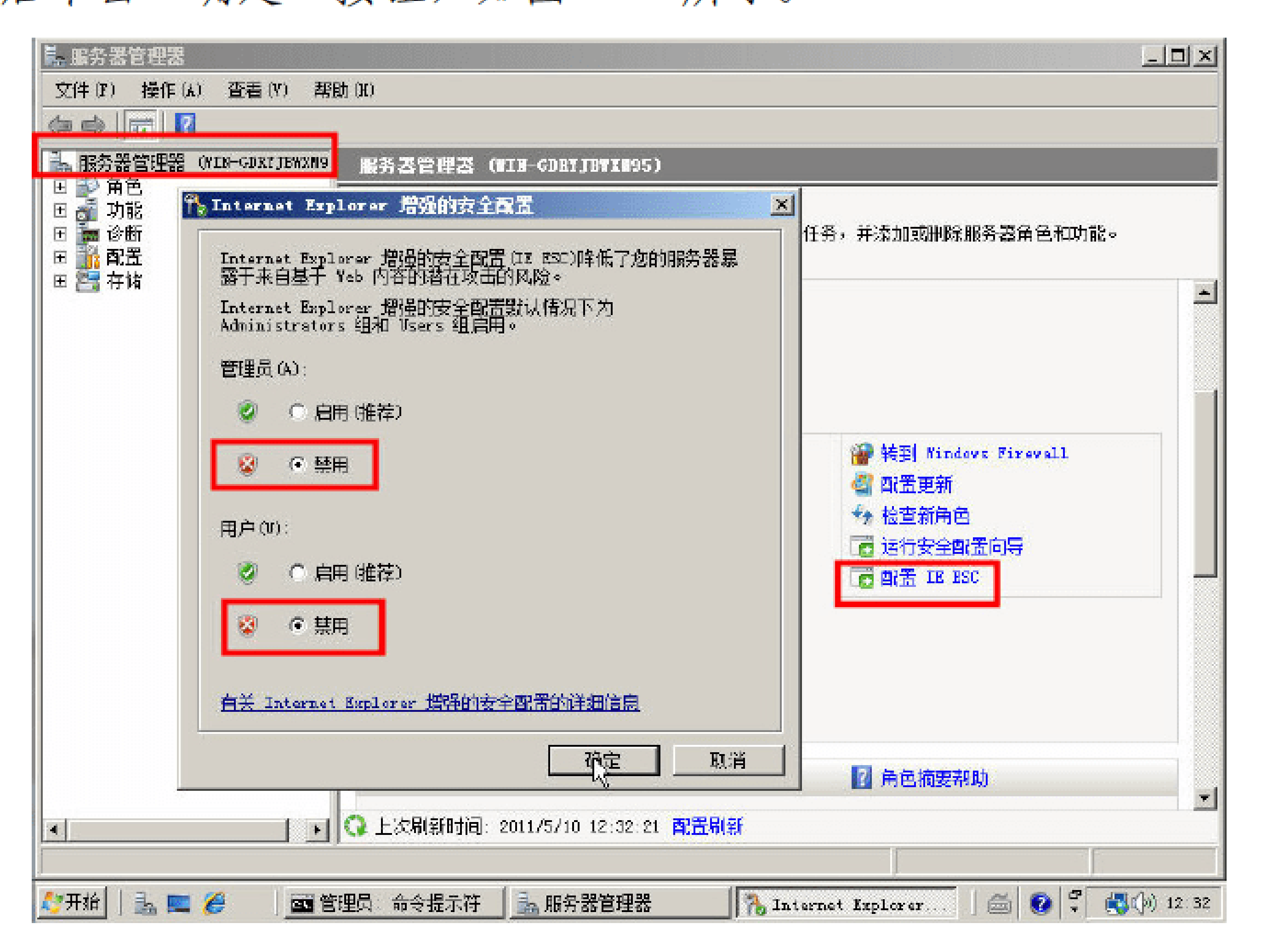


图 1-34　禁用 IE 增强的安全配置

5．激活 Windows Server 2008 R2

如果有可用的序列号，则需要激活 Windows Server 2008 R2，这样可以长期用来做各种测试。当然，即使不激活 Windows Server 2008 R2，用来做实验或者实际使用，也没有任何问题。只是在最长超过 180 天之后，每次进入系统都会提醒用户激活，但可以选择“以后激活”来继续使用。下面演示一下激活的步骤。

01 在“控制面板”中打开“系统”（也可以用鼠标右击“计算机”，在弹出的快捷菜单中选择“属性”命令进入），单击“更改产品密钥”链接，如图 1-35 所示。

02 在弹出的“Windows 激活”对话框中，输入 Windows Server 2008 R2 企业版的产品序列号，如图 1-36 所示。然后单击“下一步”按钮。



图 1-35　更改产品密钥

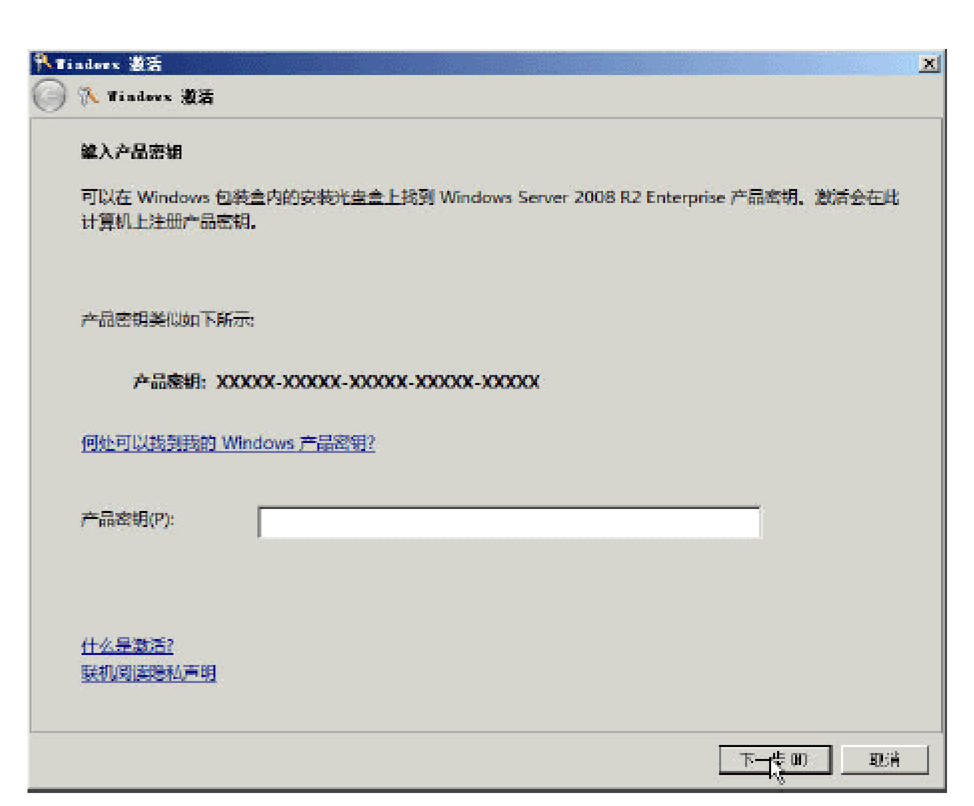


图 1-36　输入产品密钥

03 如果当前的计算机能连接到 Internet，并且输入的产品密钥在授权范围内，将会弹出“激

活成功”的提示框，如图 1-37 所示。

04 如果输入的产品密钥超过授权范围，将会出现“Windows 激活错误”的提示，如图 1-38 所示。当出现这种情况下，返回到图 1-35、图 1-36，重新输入新的密钥进行激活。

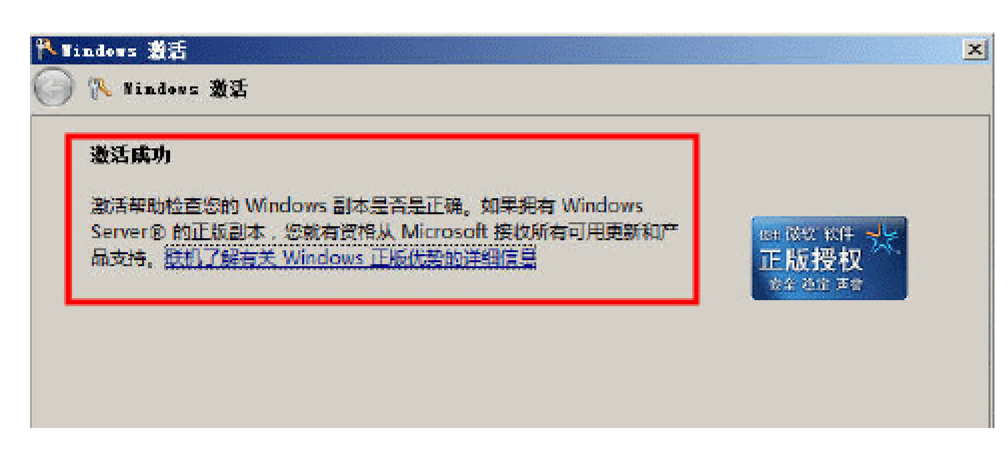


图 1-37　激活成功

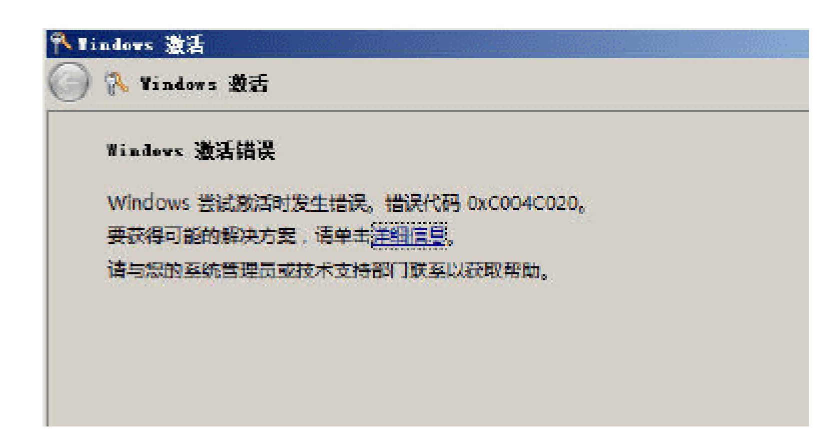


图 1-38　激活错误

05 激活成功之后，在“控制面板→系统”中，会显示“Windows 已激活”的提示，如图 1-39 所示。



图 1-39　Windows 已激活

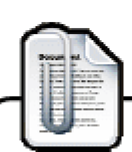


说　明

如果不想激活 Windows Server 2008 R2，又想延期使用它，可以在激活到期后，在命令提示窗口中，运行 slmgr.vbs /rearm 命令，通过重置计算机的授权状态的方法，延期使用。每运行一次 slmgr.vbs /rearm，将延长 60 天的激活期，并且可以运行三次 slmgr.vbs /rearm 命令。也可以使用 slmgr.vbs /dlv，查看剩余激活时间以及重置激活次数。

6. 安装常用软件

在 Windows Server 2008 R2 进行激活和基本配置之后，为了以后实验方便，我们将在 Windows Server 2008 R2 中，安装需要的常用软件，例如 WinRAR 程序、输入法等，但不建议在虚拟机中安装杀毒软件、监控软件。这些安装方法，与在主机系统中安装一致，不一一介绍。



说　明

如果想将安装程序“拷贝”到虚拟机中，可以直接在虚拟机中连接 Internet，使用共享文件夹等方式，获得安装程序。

7. 备份安装好的虚拟机

在以后的学习中，我们会多次使用安装、配置好的虚拟机做各种实验。实验可能会成功，也

可能会失败。当实验失败后，我们可能将 Windows Server 2008 R2 恢复到实验前的状态，也可能不能完全恢复到实验前的状态。

用户可以使用 Hyper-V 的“快照”方式，保存 Windows Server 2008 R2 虚拟机的状态，或者使用 Hyper-V 的“导出”、“导入”功能，备份虚拟机，有关这些操作，可参见本书第 11 章的相关内容。

第 2 章　Windows Server 2008 R2 基本配置

Windows Server 2008 R2 的操作与我们熟悉的 Windows XP、Windows Server 2003 相比，有较大的区别。为了全面地了解并熟悉 Windows Server 2008，本章将介绍 Windows Server 2008 R2 的基本配置，包括修改计算机名称、设置 IP 地址等设置，还将介绍 Windows Server 2008 R2 的用户与用户组管理、Windows Server 2008 R2 的防火墙设置等内容。

2.1　控制面板选项

在 Windows Server 2008 R2 的“控制面板”设置中，可以调整计算机的设置，下面将对“显示设置”、“鼠标指针”等几项进行介绍，其他项请读者自行学习。

2.1.1　鼠标指针

进入操作系统后，用鼠标右击桌面，在弹出的快捷菜单中选择“屏幕分辨率”（如图 2-1 所示），打开“控制面板→所有控制面板项→显示→屏幕分辨率”对话框，单击“所有控制面板选项”，如图 2-2 所示。

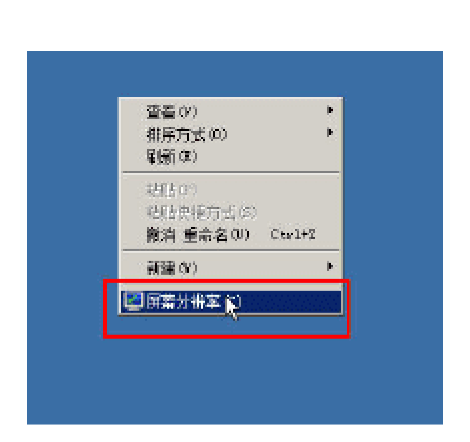


图 2-1　屏幕分辨率

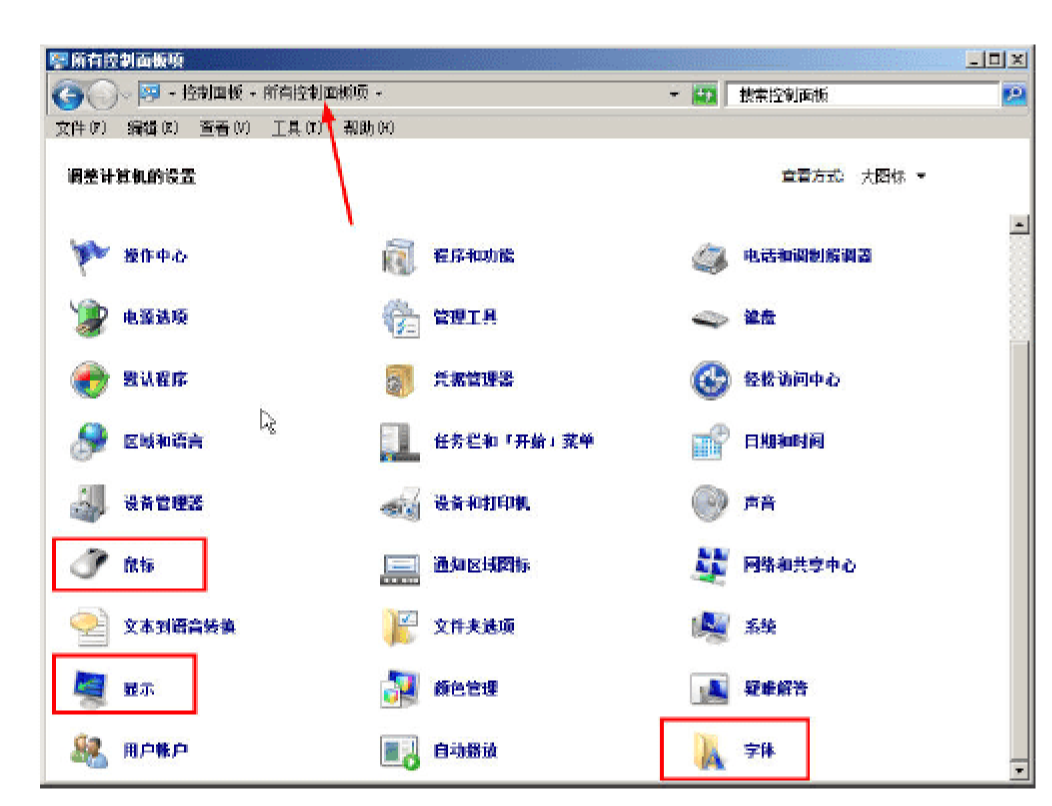


图 2-2　所有控制面板选项

在图 2-2 中，单击“鼠标”链接，将打开“鼠标 属性”对话框，在该对话框中，可以调整鼠标的移动速度、双击速度、鼠标左右键切换、鼠标的指针方案（如图 2-3 所示）、鼠标滑轮等项。

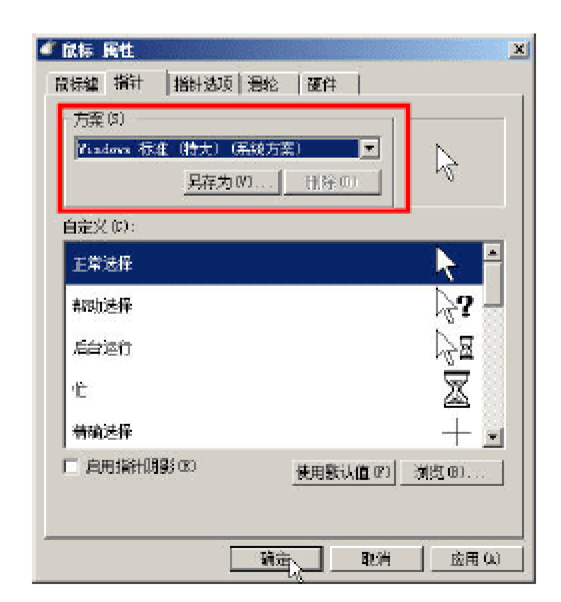


图 2-3　鼠标指针方案

2.1.2　显示设置

在图 2-2 中，单击“显示”链接，打开“显示”对话框，该对话框包括“调整分辨率”、“更改桌面背景”、“更改配色方案”、“更改屏幕保护程序”、“更改显示器设置”、“调整 ClearType 文本”、“设置自定义文本大小（DPI）”选项，如图 2-4 所示。

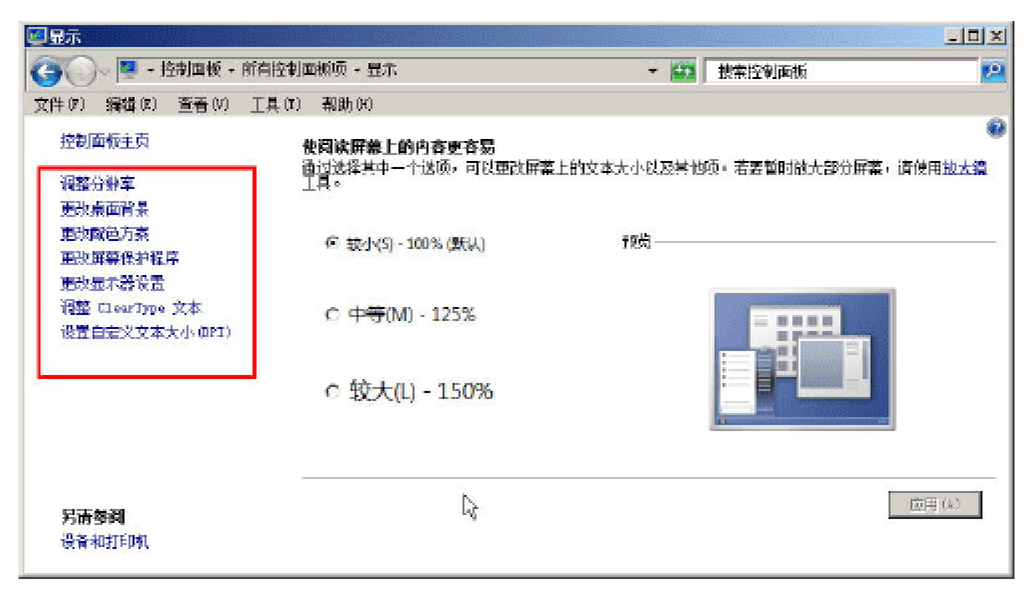


图 2-4　显示设置

单击“调整分辨率”链接，打开“屏幕分辨率”对话框，在此可以设置显示器的分辨率，如图 2-5 所示。



说 明

17 英寸和 19 英寸标准液晶显示器，其最佳分辨率为 1280×1024；20 英寸标准液晶显示器最佳分辨率为 1600×1200；20 英寸和 22 英寸宽屏液晶显示器最佳分辨率为 1600×1050；24 英寸宽屏液晶浏览器最佳分辨率为 1920×1200。

在图 2-5 中，单击“高级设置”按钮，在“监视器”选项卡中，可以调度显示器的刷新频率，如图 2-5 所示。对于液晶显示器来说，屏幕刷新频率调整为 60Hz 或 75Hz 即可；如果是 CRT 显示器，则推荐调整为 85Hz（最低为 75Hz）。

在“疑难解答”选项卡中，单击“更改设置”，在弹出的“显示适配器疑难解答”对话框中，可以调整硬件加速设置。一般情况下，将“硬件加速”状态条调整到最右侧（完全），可以获得最好的性能，如图 2-6 所示。



图 2-5　屏幕刷新频率设置

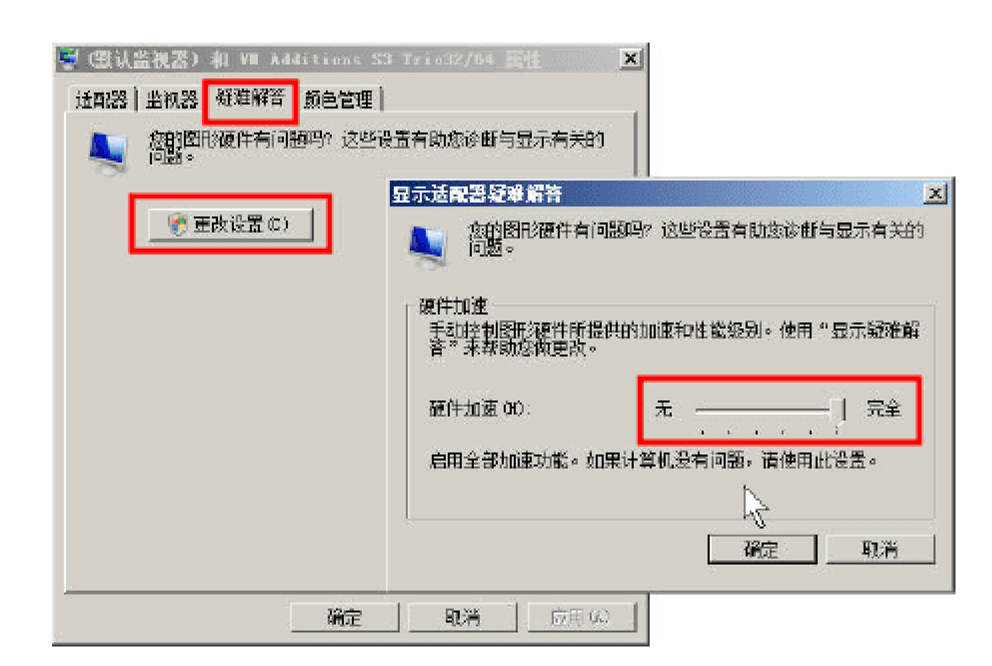
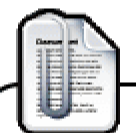


图 2-6　启用硬件加速

当计算机有多个显示器时，可以将显示桌面扩展到多个显示器上，如图 2-7 所示。也可以选择其中任意一个作为主显示器，用鼠标选中其中的一个显示桌面，通过左右、上下移动来更改显示位置。



图 2-7　多显示器



说 明

从 Windows 98 开始，Windows 即支持多个显示器。可以单独设置每个显示器的分辨率与屏幕刷新频率，也可以调整多个显示器的位置。可以在多个显示器中显示同一个界面（在“多显示器”中选择“复制这些显示”选项），或者，只在其中一个显示器上显示内容而不使用其他显示器。

2.1.3　调整字体大小

在图 2-4 中，单击“设置自定义文本大小（DPI）”链接，进入“DPI 缩放比例”对话框，默认情况下，显示为 96DPI。如果的笔记本是高分屏，要想获得更好的显示效果，可以选择“更大比例（120DPI）”，或者单击“自定义 DPI”按钮，在弹出的“自定义 DPI 设置”对话框中，缩放为正常比例的 100%、125%、150%、200%，如图 2-8 所示。



说 明

通常情况下，推荐使用“最佳分辨率”，但对于有些高分辨率显示屏的计算机来说，使用最佳分辨率后，显示字体会比较小。为了兼顾最佳分辨率与显示字体之间的问题，可以在图 2-8 所示的“自定义 DPI 设置”对话框中，通过调整 DPI 缩放比例，在最佳分辨率的基础上，获得最好的显示效果。

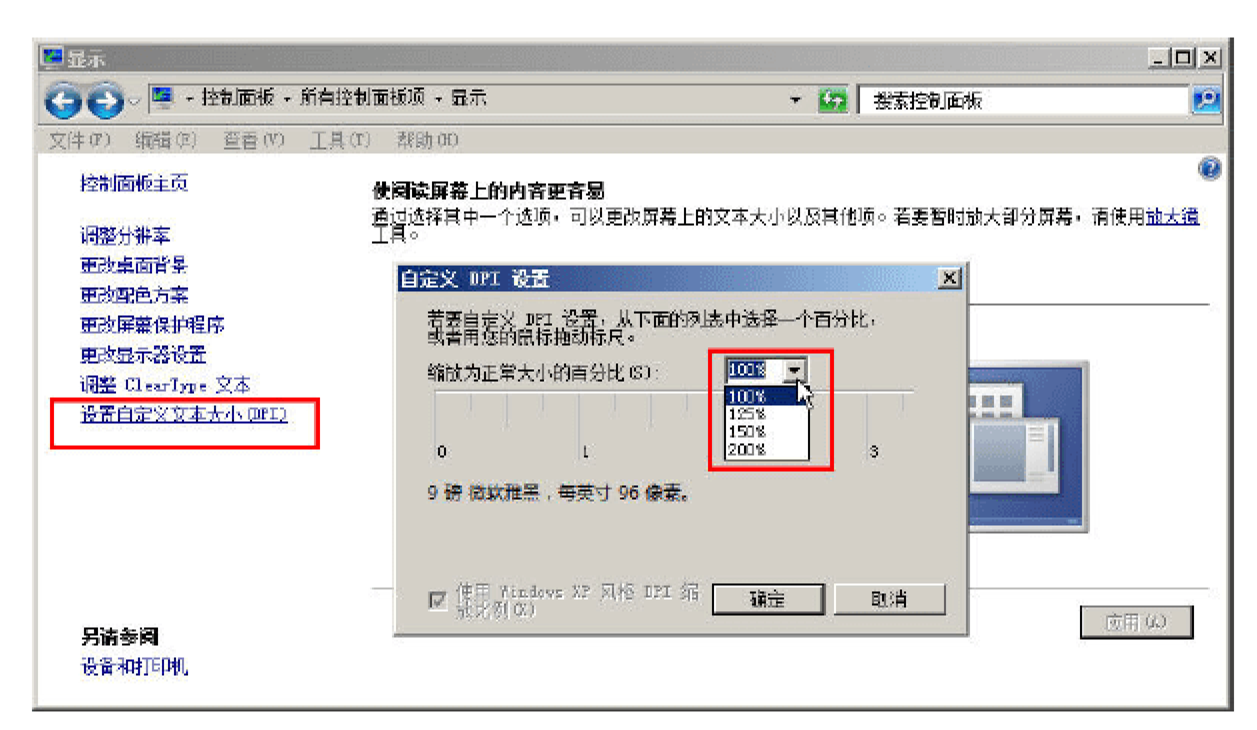


图 2-8　DPI 缩放比例

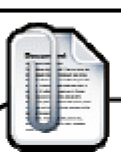
2.2　修改计算机名称与 SID

在企业网络中，需要做统一规划的有“计算机名称”、“IP 地址”、“用户名”、“用户组名”、“组织单位名称”等信息。一个规划好的网络，可以根据网络中的“计算机名称”信息，知道计算机的使用者及其所属单位及部门。

在企业网络中，可以有多种方式规划“计算机名称”。例如，如果网络规模比较小，可以直接用计算机使用者的人名的“全称”或“简称”加后缀或前缀的方式；如果网络规模比较大，可以用“部门名称”作为前缀、用使用者的人名作为后缀的方式进行命名。当有重名的时候，可以采用加序号的方式进行。例如，表 2-1 介绍了几种计算机名称的命名方式。

表 2-1　计算机名称的示例命名

部门	计算机使用者	计算机名
财务部	张三	cwb-zhangsan
人事部	李四	rsb-lisi
组织部	王五	zzb-wangwu
	张三	zhangsan
	李四	lisi
	王五	wangwu
	赵六	zhaoliu



说 明

（1）无论采用何种命名方式，计算机名称的总长度不要超过 15 个字符。

（2）在没有加入到域（Active Directory）的工作组网络中，计算机名称是“NetBIOS 名称”，该名称不能在多个 VLAN 的网络中，不能通过广播的方式获得其对应的 IP 地址，要想在 VLAN 的网络中，采用 NetBIOS 名称进行网络通信，需要在组织中配置 WINS 服务器进行解析。

（3）无论采用何种命名方式，在同一个组织内命名方式应该统一。

在 Windows Server 2008、Windows Server 2008 R2 中，修改计算机名称的步骤如下。

01 在“开始”菜单中，用鼠标右击“计算机”，在弹出的快捷菜单中选择“属性”，如

图 2-9 所示。

02 在打开的“控制面板→所有控制面板→系统”对话框中，在“计算机名称、域和工作组设置”选项组中显示了当前计算机的名称、工作组或域描述。单击“改变设置”链接（如图 2-10 所示），即可修改计算机名称。

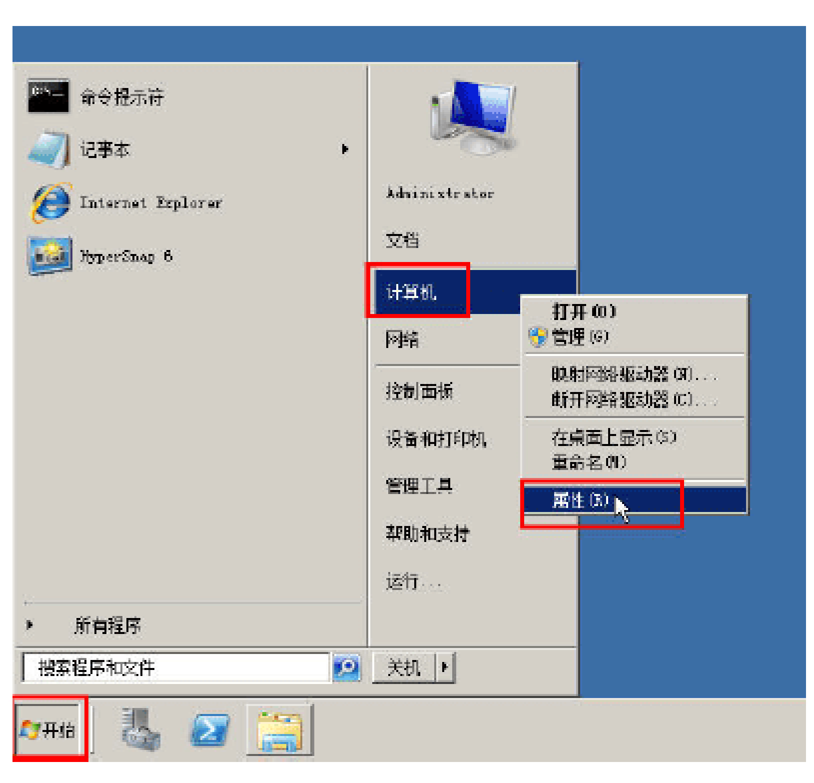


图 2-9　计算机属性

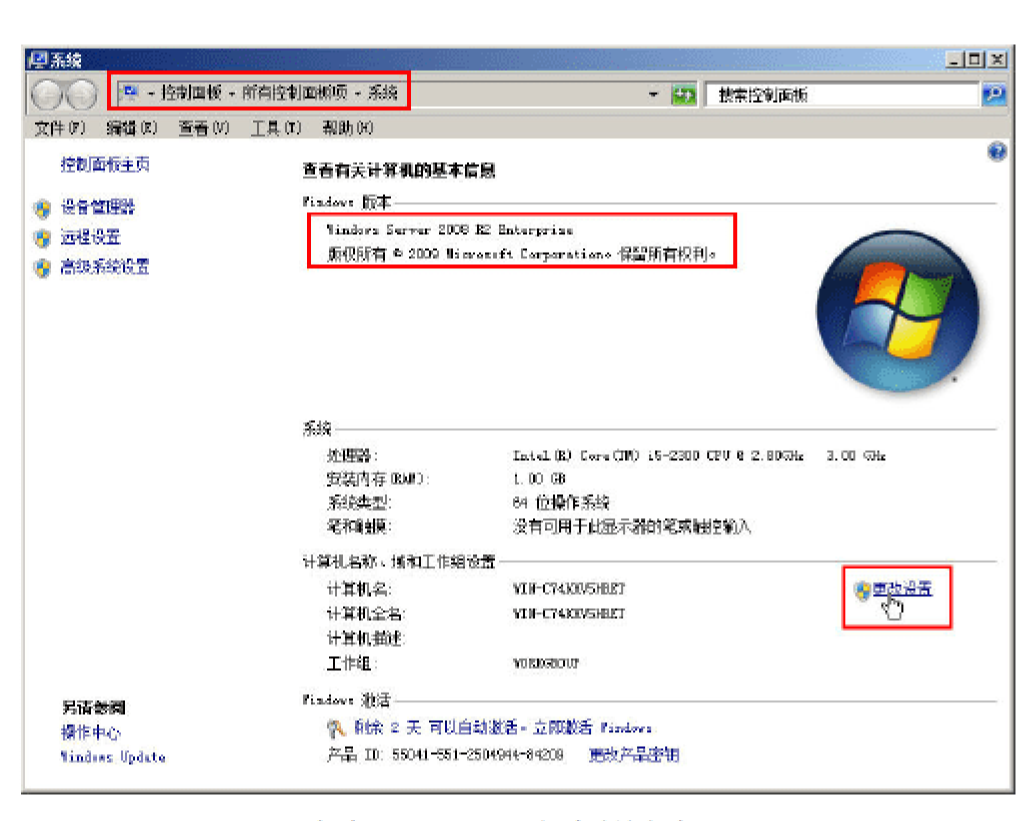


图 2-10　更改设置

03 在弹出的“系统属性”对话框中，在“计算机名”选项卡中，单击“更改”按钮，在弹出的“计算机名/域更改”对话框中，在“计算机名”文本框中，输入修改后的计算机名称（在本例中，将计算机名称修改为 ws08r2。在 Windows 系统中，计算机名称是不分大小写的），也可以在“隶属于”选项组中，修改“工作组”名称，或者将计算机加入到域。修改之后单击“确定”按钮，在弹出的“计算机名/域更改”提示框中，单击“确定”按钮，如图 2-11 所示。

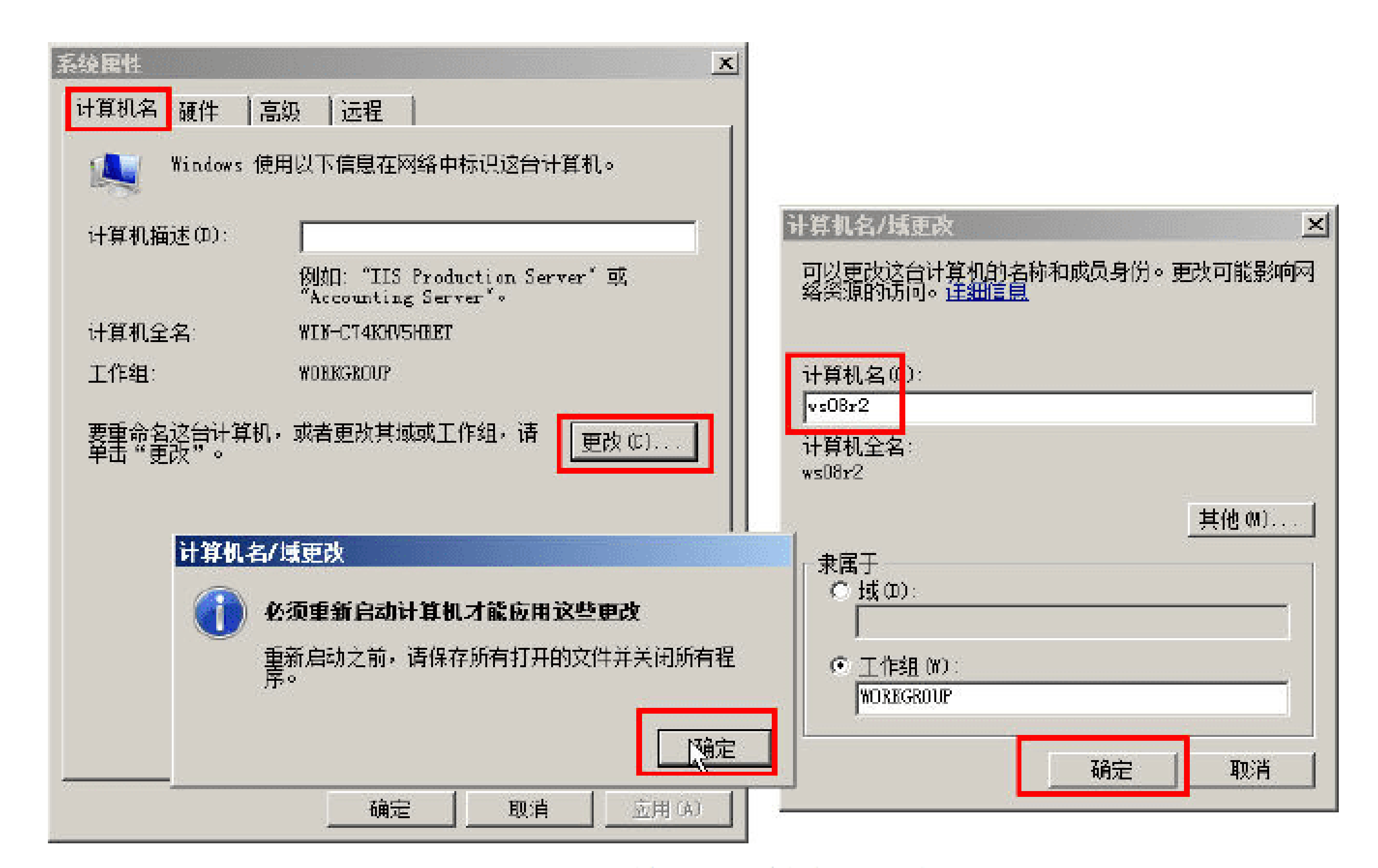
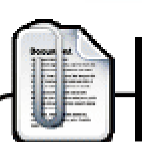


图 2-11　修改计算机名称

04 修改计算机名称后，根据提示，重新启动计算机。



说　明

如果想修改计算机名称，并且将计算机加入到域，可在修改计算机名称后，重新启动计算机，再次进入系统后，完成“将计算机加入到域”的操作。如果在修改计算机名称后，同时完成“将计算机加入到域”的操作，计算机会将旧的名称加入到域，这样就达不到我们的要求了。

目前，主机虚拟化是一个“主流”的应用。在采用虚拟化技术之后，使用虚拟化管理工具，从一个“模板”虚拟机，可以轻易地复制出多台相同的 Windows Server 2008 或 Windows 7 操作系统。如果复制的多台 Windows Server 2008 或 Windows 7 是分别用于不同的网络，不会有任何问题的。如果复制的多台 Windows Server 2008 或 Windows 7 用于相同的网络，并且都要加入到 Active Directory，由于这些克隆出来的计算机具有相同的 SID，则会造成网络问题。为了避免这个问题，需要在克隆后的计算机中，通过运行 sysprep 程序，以重新生成 SID。Windows 2008、Windows Vista 之后的系统，在安装的时候，已经集成了 sysprep 程序，可以打开命令提示符窗口，进入 c:\windows\system32\sysprep 文件夹，通过执行 sysprep /generalize，重新生成 SID，这样复制后的计算机，再加入到 Active Directory 就不会有任何问题了，如图 2-12 所示。

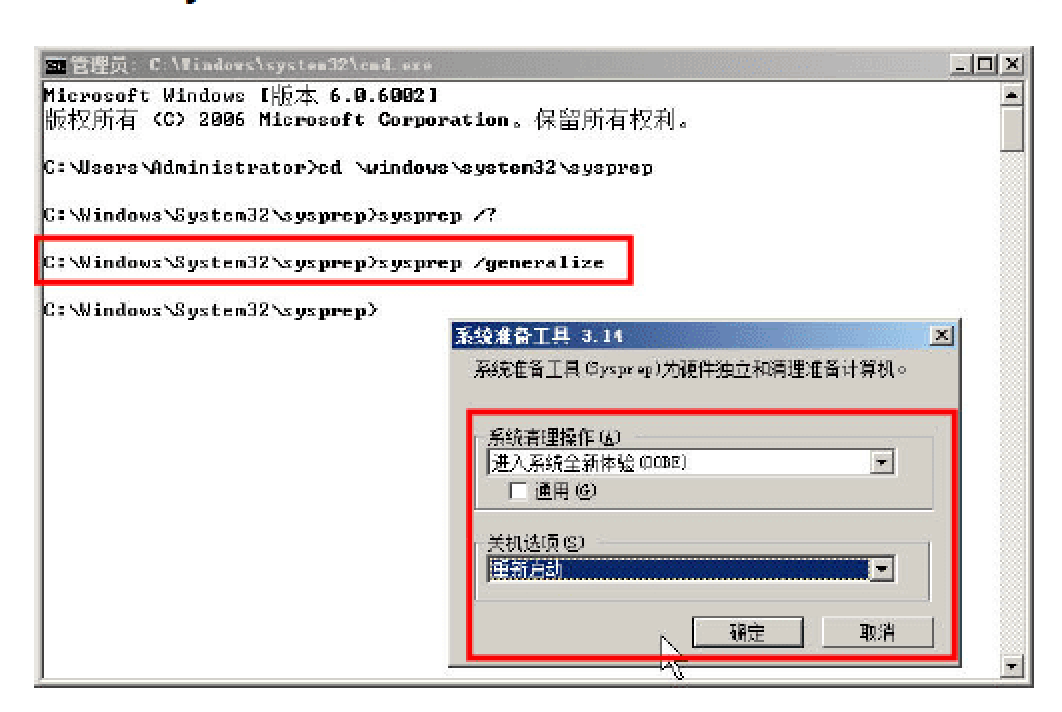


图 2-12　运行 sysprep 重新生成 SID



说 明

在运行 sysprep 之后，原来已经激活的系统（在复制前已经激活、在复制之后仍然是激活的状态），需要重新激活。

2.3　IP 地址与多网络设置

在网络中，需要对 IP 地址、子网掩码进行统一的规划。对于企业网络来说，通常使用私有的 IP 地址段，即 10.0.0.0/8、172.16.0.0/12、192.168.0.0/16 的地址范围，并且根据需要，做进一步的子网划分。一般情况下，如果管理一个网络，可以使用上述三个地址范围中的一部分，对整个网络做出规划。如果网络已经规划好，则可以根据规划的内容，对新加入到网络中的服务器、工作站，进行合理的配置，这包括 IP 地址、子网掩码、网关、DNS、WINS 服务器等相关参数的设置。

2.3.1　修改或设置 IP 地址

在安装完 Windows Server 2008 后，其默认情况是“自动获得 IP 地址”与“自动获得 DNS 服务器地址”。当网络中有 DHCP 服务器时，可以自动从网络中获得 IP 地址、子网掩码，DNS、WINS 服务器地址等参数。如果网络中没有 DHCP 服务器，或者虽然存在 DHCP 服务器，但想要为服务器指定一个“静态”的 IP 地址，可以手动设置 IP 地址。在 Windows Server 2008 中，指定 IP 地址的操作步骤如下。

01 单击屏幕右下角系统状态栏中的“ ”，在弹出的快捷菜单中选择“打开网络和共享中心”选项，如图 2-13 所示。

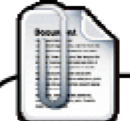
02 在“网络和共享中心”窗口中，在“网络”选项组中，单击“本地连接”命令（如图 2-14 所示），在弹出的“本地连接 状态”对话框中，单击“属性”按钮。



图 2-13　网络和共享中心



图 2-14　查看状态



说 明

如果想修改网络连接的名称、启用或禁用网卡，可以在图 2-14 中，单击“更改适配器设置”链接，将会打开“网络连接”窗口，在此窗口中，可以重命名网卡名称、启用或禁用网卡，如图 2-15 所示。这相当于以前的 Windows XP、Windows Server 2003 中，用鼠标右击桌面上的“网上邻居”，在弹出的快捷菜单中选择“属性”选项。

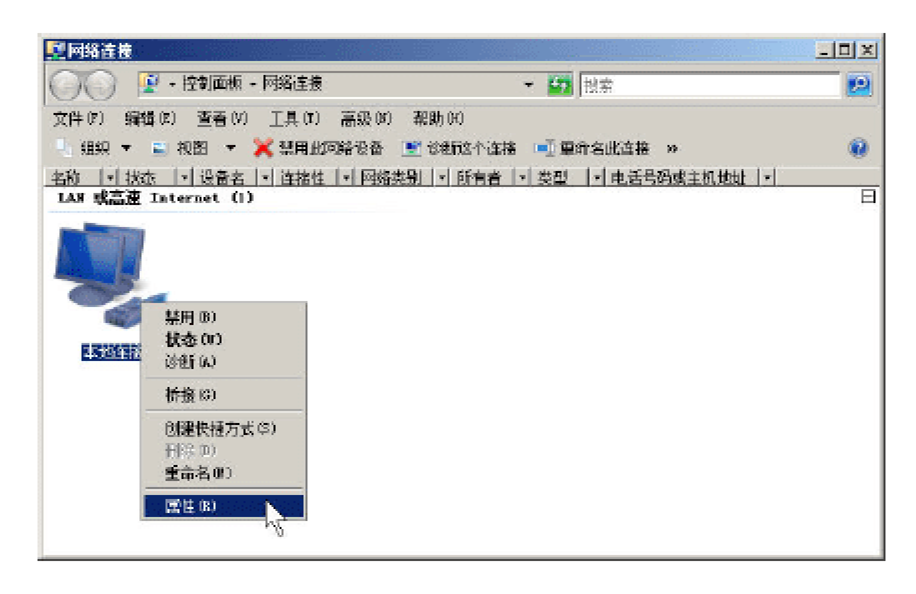


图 2-15　网络连接

03 在弹出的“本地连接 属性”对话框中，选中“Internet 协议版本 4（TCP/IPv4）”，单击“属性”按钮，在弹出的“Internet 协议版本 4（TCP/IPv4）属性”对话框中，可以设置 IP 地址获得方式为“自动获得 IP 地址”与“自动获得 DNS 服务器地址”；也可以选择“使用下面的 IP 地址”与“使用下面的 DNS 服务器地址”的方式，指定 IP 地址、子网掩码、网关与 DNS 地址，如图 2-16 所示。

04 如果需要为当前的网卡设置多个 IP 地址、多个 DNS 服务器的地址（多于 2 个），或者需要指定 WINS 服务器的地址，可以在图 2-16 所示的对话框中，单击“高级”按钮，在弹出的“高级 TCP/IP 设置”对话框中进行配置，如图 2-17 所示。

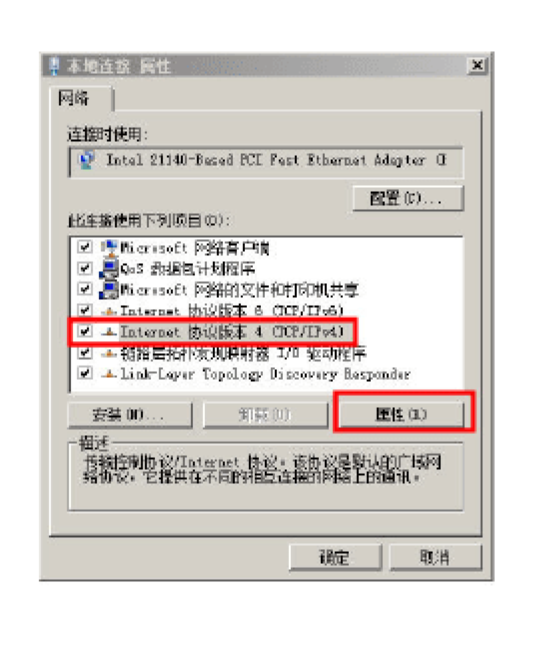
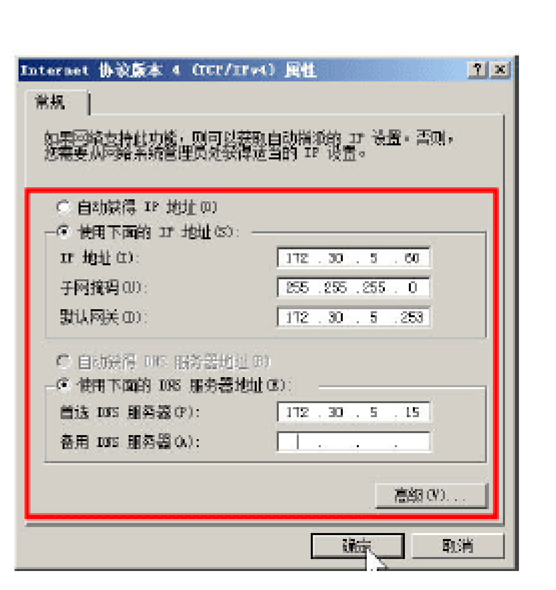



图 2-16　指定 IP 地址相关参数

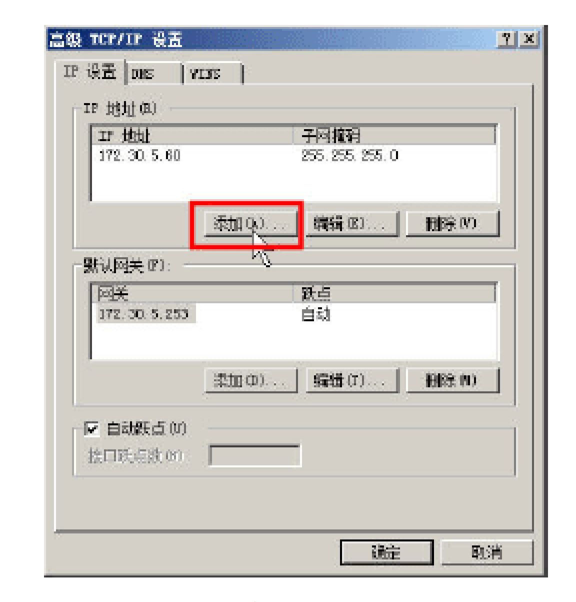
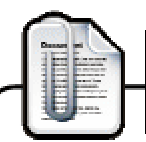


图 2-17　高级 TCP/IP 设置



说 明

在图 2-17 所示对话框中，虽然也可以添加多个网关，但不建议在该对话框中添加，在此添加多个网关会引发通信问题，有关“多网络、多网关”的内容，可参见“2.3.3 多网络设置”一节内容。

05 在设置之后，依次单击“确定”按钮返回。

2.3.2 备用网络设置

如果是在笔记本或其他便携式的计算机上安装 Windows Server 2008 R2，并且需要在多个网络中切换时，如果需要切换的多个网络，都配置有 DHCP 服务器，则计算机只需要设置成“自动获得 IP 地址”与“自动获得 DNS 服务器地址”即可（如图 2-18 所示），如果要切换的多个网络，有的网络中配置 DHCP 服务器，有的网络需要指定静态的 IP 地址，就可以使用 Windows Server 2008 中的“备用配置”功能来解决这个问题。在下面的操作中，假设安装 Windows Server 2008 操作系统的笔记本中，一个网络配置有 DHCP 服务器，另一个网络中需要指定 IP 地址（本例为 172.30.5.60、网关为 172.30.5.253、DNS 为 172.30.5.15），备用配置的设置方法如下。

01 参照上文的操作步骤，进入“Internet 协议版本 4（TCP/IPv4）属性”对话框，在“常规”选项卡中，选择“自动获得 IP 地址”与“自动获得 DNS 服务器地址”，如图 2-18 所示。

02 在“备用配置”选项卡中，设置另一个网络需要指定的静态 IP 地址、子网掩码、网关和 DNS 服务器地址，如图 2-19 所示。设置完成后单击“确定”按钮即可。

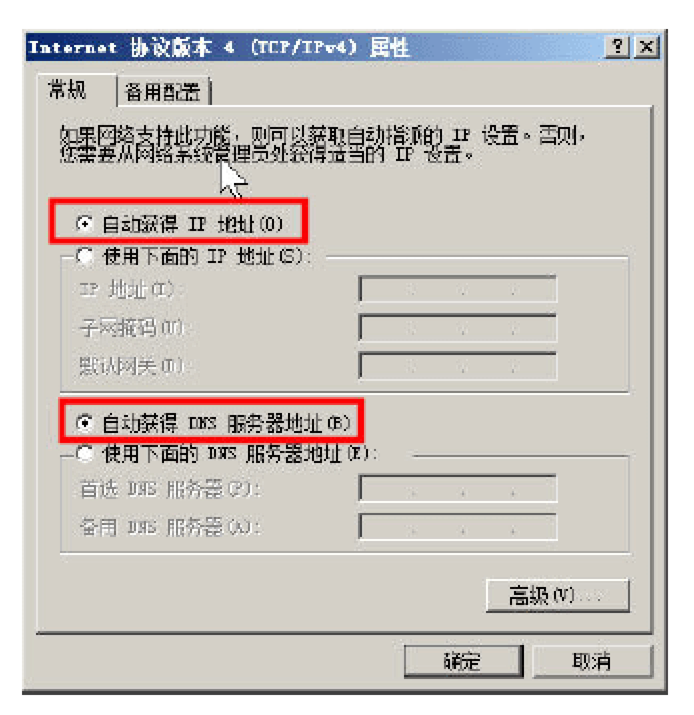


图 2-18　自动获得地址

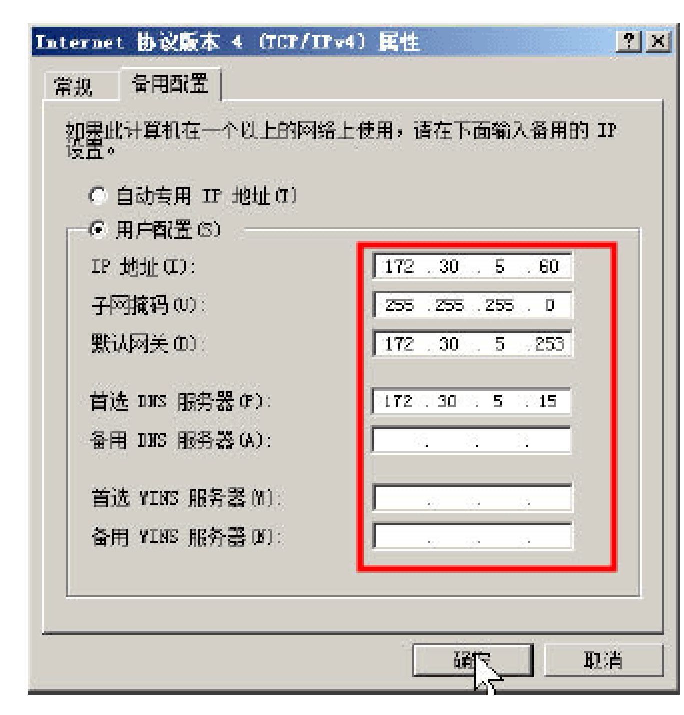


图 2-19　备用配置

2.3.3　多网络设置

在很多时候，计算机可能连接到不止一个网络，并且每个网络都有网关地址，这时候，如果用普通的方法，在图形界面中，添加多个网关地址，是不能同时连接到各个网络的。在这种情况下，可以使用 route 命令，通过添加静态路由的方式，添加到不同网络，以达到同时连接到多个网络的目的。为了让大家有个直观的认识，我们通过图 2-20 所示的网络拓扑，分析这个问题。

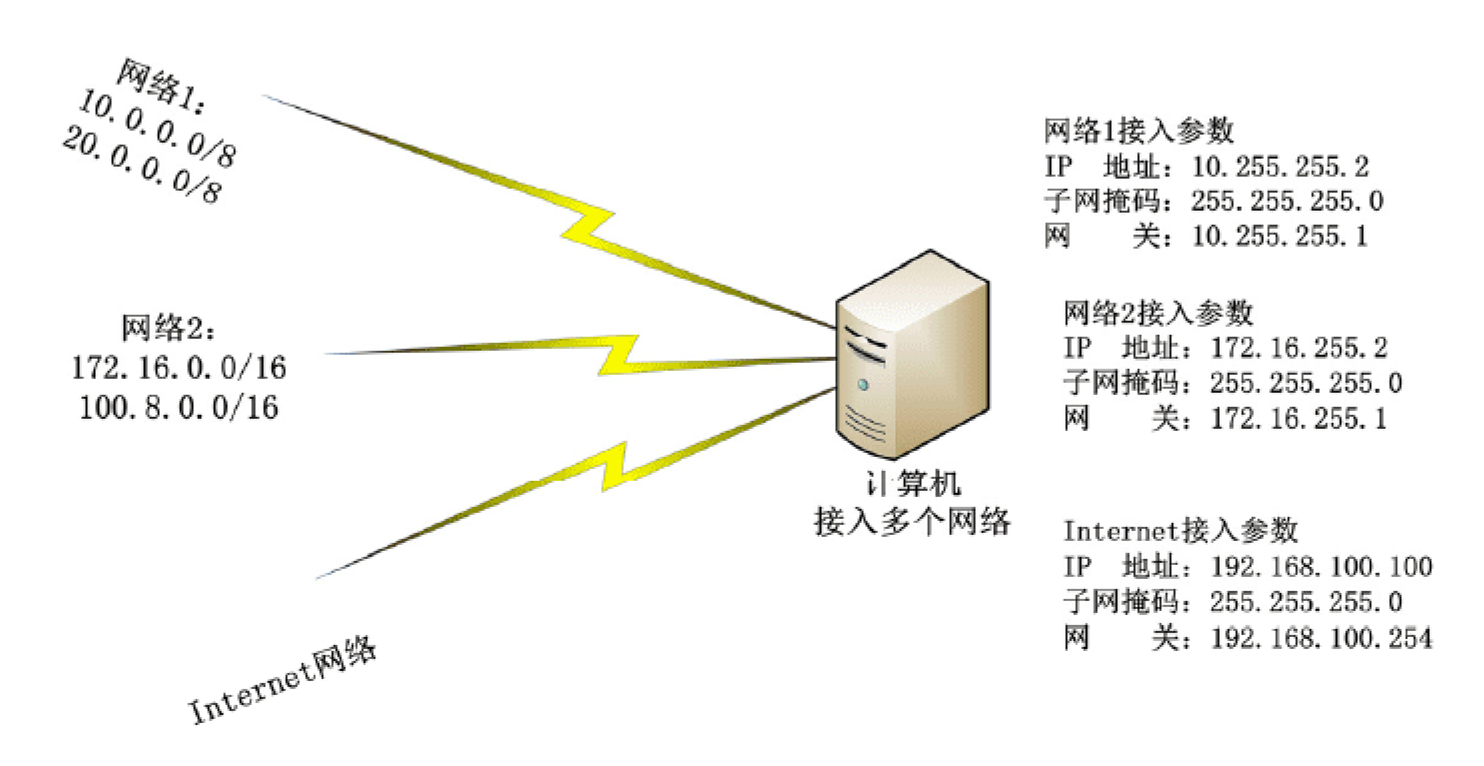


图 2-20　接入多网络

在图 2-20 中，有一台计算机同时连接到多个网络。这台计算机可以使用 1 个网卡，也可以使用 2 个或 3 个网卡，分别接入多个不同的网络。

如果使用 1 个网卡接入 3 个网络，可以根据图 2-17 所示的示意图，添加 3 个 IP 地址、对应的子网掩码以及 Internet 接入参数中的网关地址（作为默认网关），如图 2-21 所示。然后在命令提示符中，输入如下命令：

```
route  add  –p  10.0.0.0    mask  255.0.0.0    10.255.255.1
route  add  –p  20.0.0.0    mask  255.0.0.0    10.255.255.1
route  add  -p  172.16.0.0  mask  255.255.0.0  172.16.255.1
route  add  -p  100.8.0.0   mask  255.255.0.0  172.16.255.1
```

命令效果如图 2-22 所示。

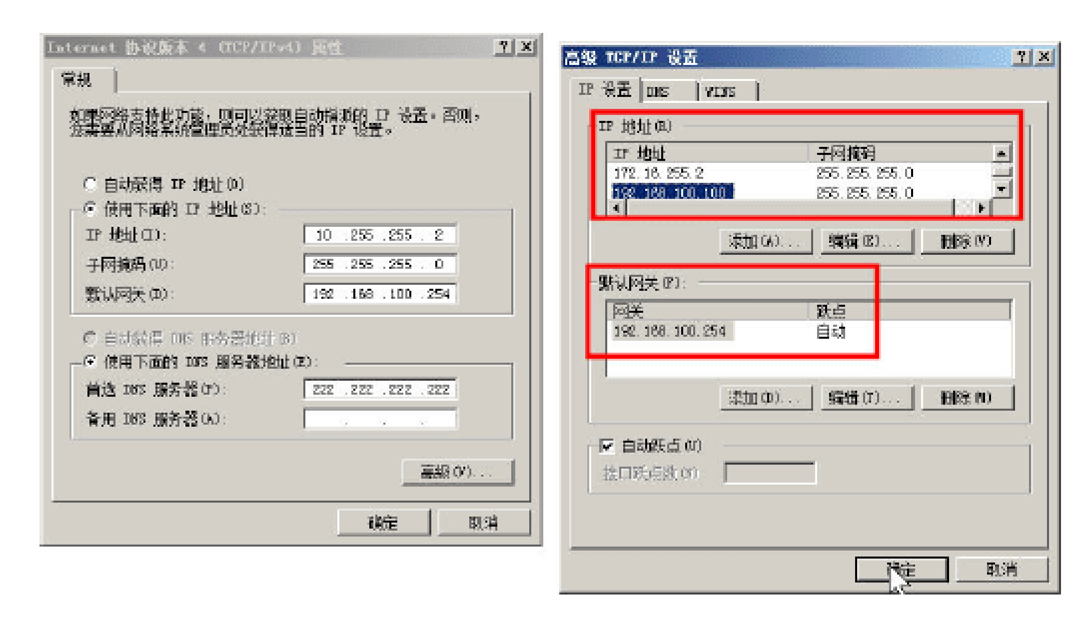


图 2-21　设置 IP 地址与网关

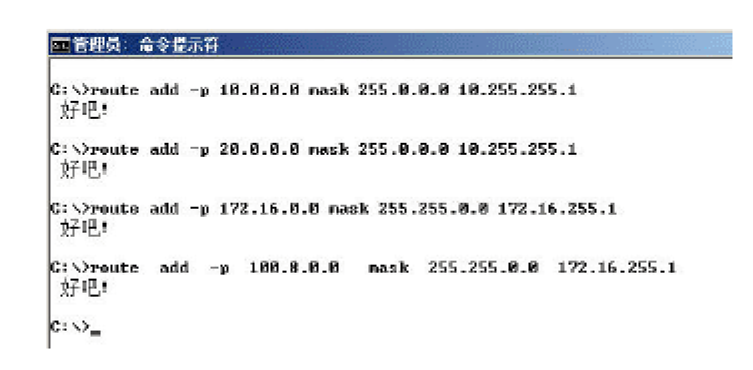


图 2-22　添加到其他网段的静态路由

在添加静态路由后，可以使用 route print 命令，查看已经添加的静态路由，如图 2-23 所示。也可以使用 ipconfig 命令，查看当前计算机添加的多个 IP 地址，如图 2-24 所示。

```
永久路由:
  网络地址          网络掩码    网关地址   跃点数
          0.0.0.0          0.0.0.0  192.168.100.254    默认
         10.0.0.0        255.0.0.0    10.255.255.1        1
         20.0.0.0        255.0.0.0    10.255.255.1        1
       172.16.0.0      255.255.0.0    172.16.255.1        1
        100.8.0.0      255.255.0.0    172.16.255.1        1
```

图 2-23　显示添加的静态路由

```
C:\>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   IPv4 地址 . . . . . . . . . . . . : 10.255.255.2
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   IPv4 地址 . . . . . . . . . . . . : 172.16.255.2
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   IPv4 地址 . . . . . . . . . . . . : 192.168.100.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.100.254
```

图 2-24　显示 IP 地址

如果添加的静态路由有误，或者需要修改静态路由，可以使用 route delete 命令，删除添加的静态路由。例如，可以使用 route delete 100.8.0.0 命令，删除到 100.8.0.0/16 的静态路由。

如果计算机使用多个网卡接入多个网络，则设置的方法与使用单个网卡接入多个网络相差不多，只需要在对应的网卡上设置对应的 IP 地址，然后在进入命令提示窗口中，使用 route 命令添加到其他网段的静态路由即可。例如，在图 2-20 的计算机上，有 3 个网卡，其中网卡 1 接入网络 1、网卡 2 接入网络 2、网卡 3 接入 Internet，则在网卡 1 上设置 IP 地址为 10.255.255.2、子网掩码为 255.255.255.0，在网卡 2 上设置 IP 地址为 172.16.255.2、子网掩码为 255.255.255.0，在网卡 3 设置 IP 地址为 192.168.100.100、子网掩码为 255.255.255.0、网关地址为 192.168.100.254，并设置 DNS 服务器地址即可。这些不再一一介绍。

当然，网络的接入方式可能会有更多种。例如，在图 2-20 中，计算机有 2 个网卡，其中网卡 1 分别接入网络 1、网络 2，网卡 2 接入 Internet，则只需要在网卡 1 上设置 10.255.255.2/24、172.16.255.2/24 的地址，在网卡 2 上设置接入 Internet 的参数，然后再在命令窗口中，使用 route 命令添加到网络 1、网络 2 的静态路由即可。

2.4　Windows 防火墙设置

Windows Server 2008 R2（Windows 7 与此类似）的 Windows 防火墙设置包括“高级共享设置”、“基本防火墙”与“高级防火墙”、“网络位置”几部分的内容，下面分别进行介绍。

2.4.1　高级共享设置

打开“网络和共享中心”，单击“高级共享设置”，如图 2-25 所示。



图 2-25　共享和发现

在高级共享设置中，包括不同的组，例如“家庭或工作”、“公用”，在每个组后面单击“▼”可以展开对应的项并进行设置，展开之后“▼”变为“▲”，单击该按钮可以将展开的项进行收起。

（1）在“网络发现”中可以选择“启用网络发现”或“关闭网络发现”，设置之后单击“保存修改”按钮以应用，如图 2-26 所示。

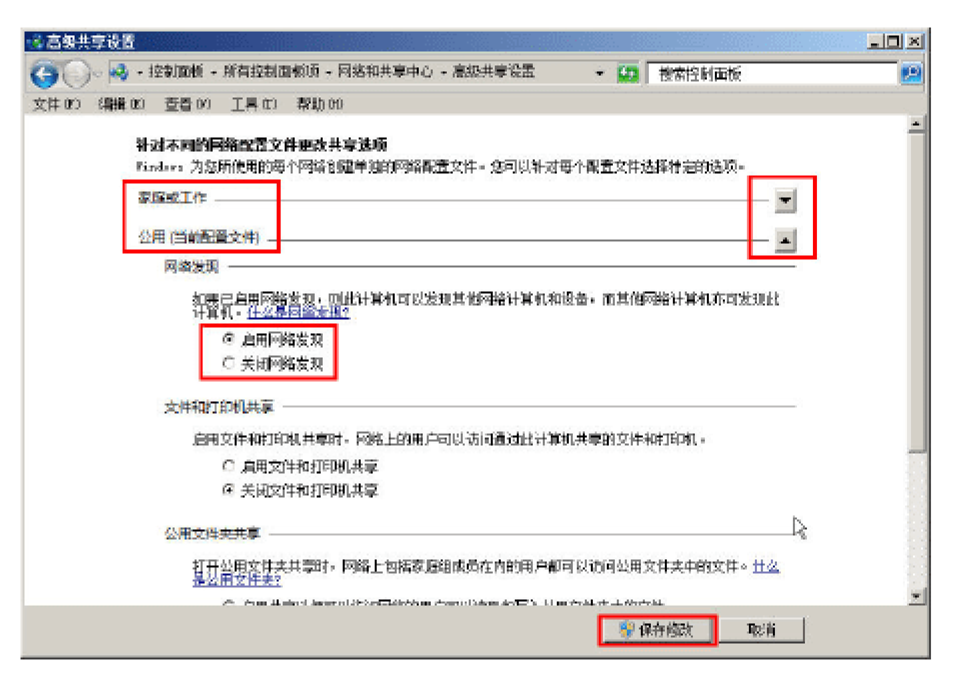


图 2-26　网络发现

“网络发现”是一种网络的设置，该设置会影响计算机是否可以查看（找到）网络上的其他计算机及其设置，以及网络上的其他计算机是否可以查看该计算机。“网络发现”有两种状态，分别是“启用”和“关闭”，各状态的意义如下。

- 启用：此状态允许当前计算机查看其他网络计算机和设备，并允许其他网络计算机上的人查看当前计算机。这使共享文件和打印机变得更加容易。
- 关闭：此状态阻止当前计算机查看其他网络计算机和设备，并阻止其他网络计算机上的用户查看当前计算机。

（2）文件和打印机共享：在启用“文件和打印机共享”时，网络上的用户可以访问从此计算机共享的文件和打印机。

（3）公用文件夹共享：如果启用“公用”文件夹共享，则网络上的用户可以访问该公用文件夹中的文件，如图 2-27 所示。

如果要查找“公用”文件夹的位置，可以从“开始”菜单选择“文档”，在左侧的任务窗格中找到 “公用图片”、“公用文档”、“公用下载”与“公用音乐”等，如图 2-28 所示。

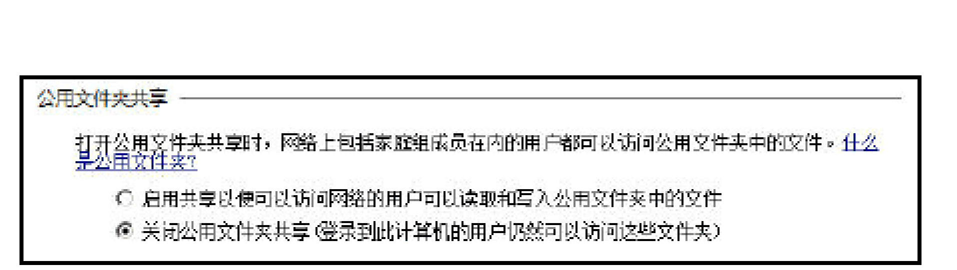


图 2-27　公用文件夹共享

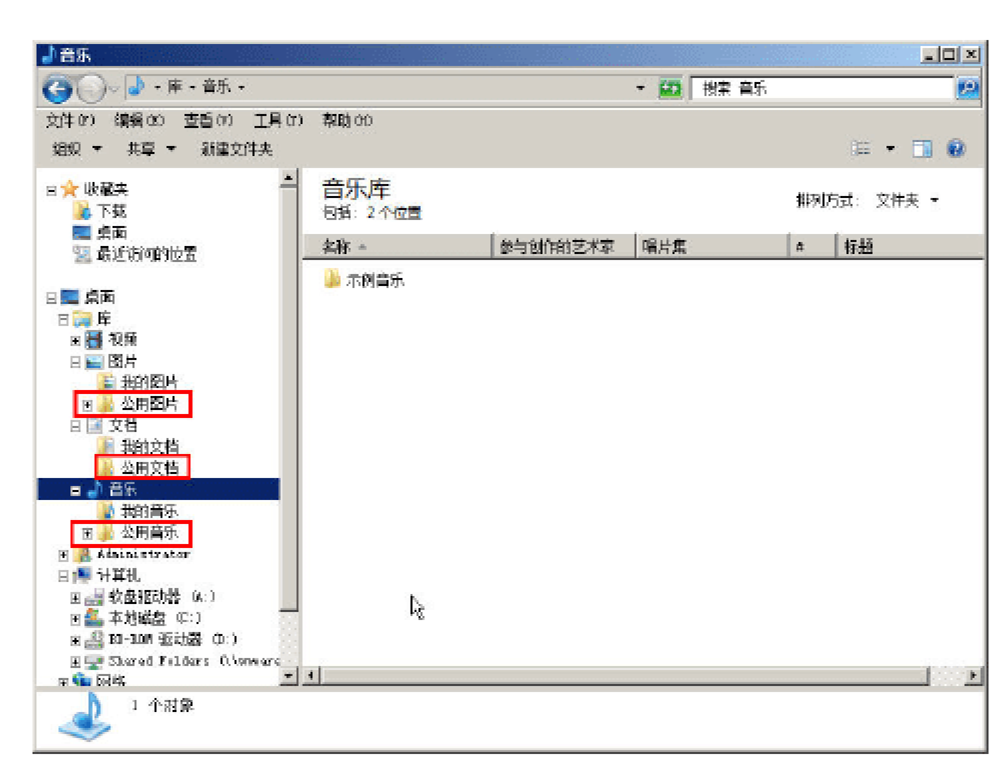


图 2-28　公用文件夹

（4）在“密码保护的共享”中，选择是否启用密码保护。如果启用密码保护，则只有具备此计算机账户和密码的用户才可以访问共享文件、连接到此计算机的打印机，以及公用文件夹。如果要使其他用户具备访问权限，则需要关闭密码保护。

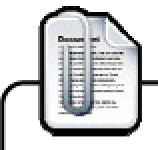
2.4.2　网络位置

第一次连接到网络，或者网络参数做出变动（例如更改 IP 地址）时，必须选择网络位置。这将为所连接网络的类型自动进行适当的防火墙设置。根据选择的网络位置，Windows 为网络分配一个网络发现状态，并为该状态打开合适的 Windows 防火墙端口。

在 Windows Server 2008、Windows Server 2008 R2 服务器产品中，有三个网络位置：专用、公用、域。在 Windows Vista、Windows 7 等工作站操作系统中，也有三个网络位置：家庭、办公室和公共场所。

（1）家庭或办公室：如果用户认识并信任网络上的人和设备，则为家庭或小型办公网络选择以上位置中的任一位置。默认情况下，网络发现处于启用状态，它允许用户查看网络上的其他计算机和设备并允许其他网络用户查看当前的计算机。

（2）公共场所（公用网络）：为公共场所（如咖啡店或机场）中的网络选择此位置。此位置旨在使当前计算机对周围的计算机不可见，并且帮助保护计算机免受来自 Internet 的任何恶意软件的攻击。对此位置禁用网络发现。



说 明

如果网络上只有一台计算机并且无须共享文件或打印机，则最安全的选择是“公共场所”。

（3）专用网络：专用网络会启用“网络搜索”功能，让该计算机找到此网络上的其他计算机，同时会通过“Windows 防火墙”的设置，开放“传入的网络搜索”端口，让其他用户在网络上浏览到该计算机。

（4）域网络：加入域的计算机的网络位置会自动设置为“域网络”，并且无法自行更改。

更改网络位置类型及网络名的步骤如下。

01 打开“网络和共享中心”，在“网络和共享中心”列表中，显示了当前计算机所处的网络，以及设置的网络名称，如图 2-29 所示。在“查看活动网络”选项组的网络名称中，单击已经选中的网络位置链接，将会打开“设置网络位置”对话框。

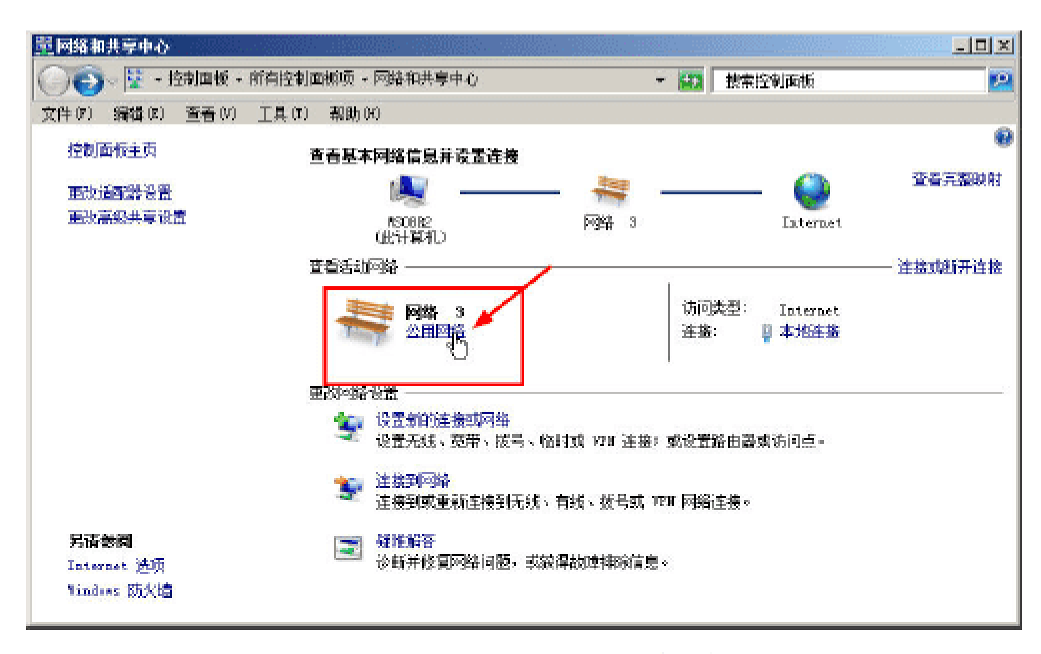
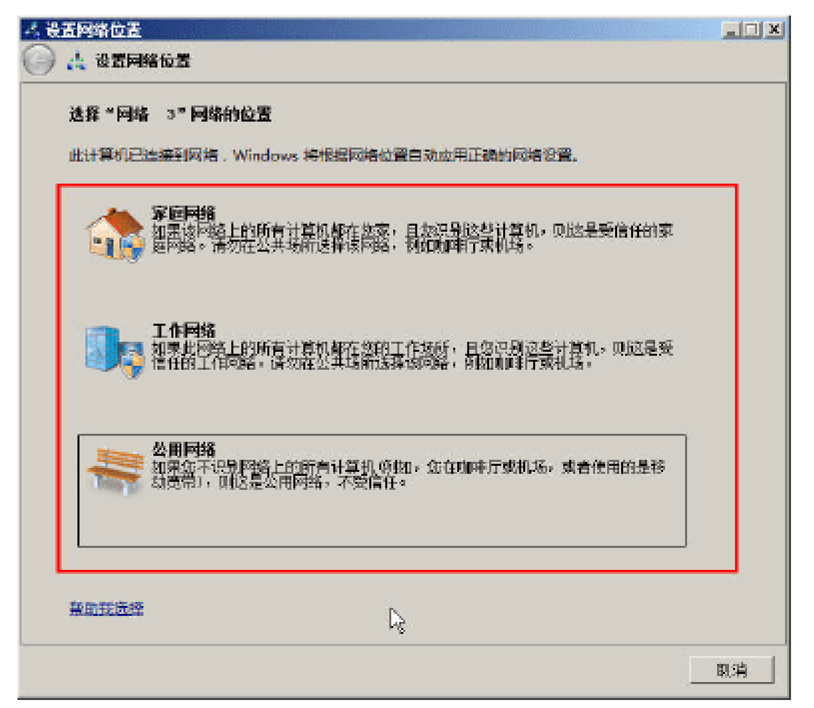


图 2-29　网络和共享中心

02 在“设置网络位置”对话框中，输入选择新的网络位置如图 2-30 所示。

03 更改完成之后，显示“网络位置现在为‘专用’”，如图 2-31 所示。单击“关闭”按钮，完成修改。



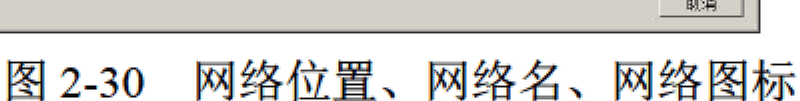


图 2-30　网络位置、网络名、网络图标



图 2-31　网络位置

04 修改之后，返回到“网络和共享中心”窗口，可以看到，网络位置与名称已经更改，如图 2-32 所示。



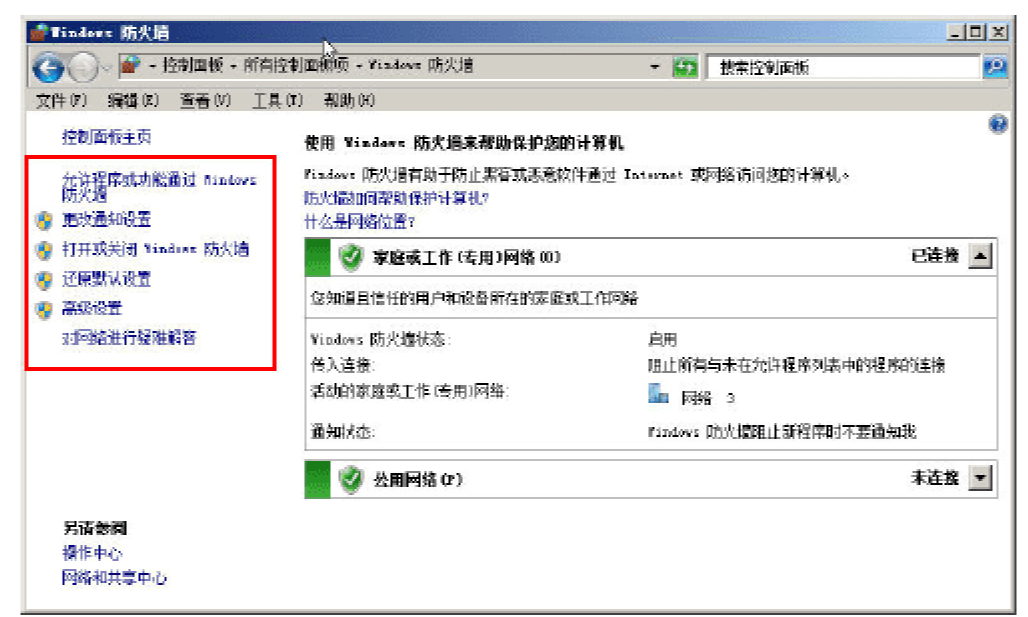
图 2-32　网络和共享中心

2.4.3　基本防火墙设置

在默认情况下，Windows Server 2008 R2、Windows 7 等操作系统，已经启用了“Windows 防火墙”，该防火墙属于“基本防火墙”，它会阻止网络上的其他计算机与此台计算机通信。

在“网络和共享中心”窗口中，在左下角单击“Windows 防火墙”选项将打开“Windows 防火墙”窗口，在该防火墙设置中，主要包括“打开或关闭 Windows 防火墙”、“允许程序或功能通过 Windows 防火墙”、“更改通知设置”、“高级设置”等几项，如图 2-33 所示。下面一一介绍。

01 在图 2-33 中，单击“打开或关闭 Windows 防火墙”或“更改通知设置”链接，打开“自定义每种类型的网络位置”对话框，在此可以为每个网络位置“启用”或“关闭”Windows 防火墙，如图 2-34 所示。



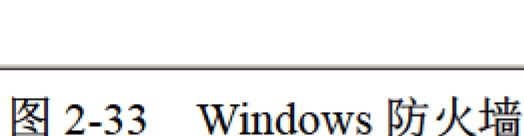


图 2-33　Windows 防火墙

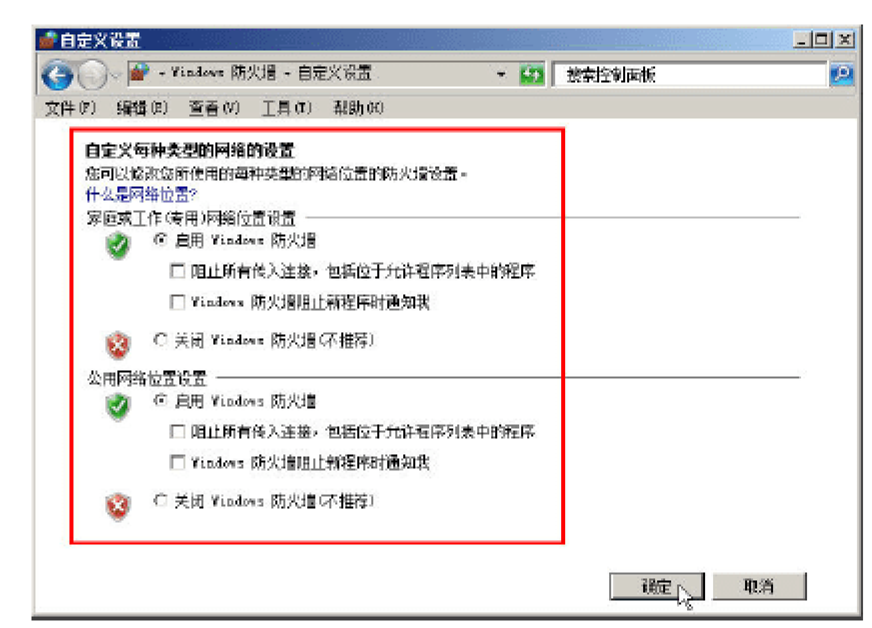
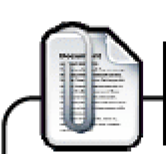


图 2-34　打开或关闭 Windows 防火墙设置

02 在图 2-33 中，单击“允许程序或功能通过 Windows 防火墙”链接，将打开“允许程序通过 Windows 防火墙通信”对话框，在此可以为当前计算机，“启用”或“禁用”系统中已经存在的“程序”或“端口”（这些端口都是允许外网访问本计算机的“入站”连接，如“网络发现”、“文件和打印机共享”、“远程桌面”等），如果启用某项，只要在某项前面的方格中用鼠标单击，并显示✓提示即为选中，没有✓即为禁用，如图 2-35 所示。



图 2-35　例外



说 明

在“Windows 防火墙”中已经添加了多种服务（端口），可以在图 2-35 所示的选项卡中，单击右侧的滑动条查看更多的服务。

如果用户的服务器是 Windows Server 2008，在“Windows 防火墙设置”中，需要为当前计算机开启一个“Windows 防火墙”不存在的服务端口，操作步骤如下。

01 打开“Windows 防火墙→允许程序通过 Windows 防火墙通信”选项卡，单击“添加端口”按钮，在弹出的“添加端口”对话框中，输入新添加的服务的名称、开放的端口号（1～65535）、开放协议（TCP 或 UDP），如图 2-36 所示。

02 如果要限制“源网络”的客户端计算机，可以选中一项服务，单击“更改范围”按钮，在弹出的“更改范围”对话框中，设置源计算机或源网络，“任何计算机（包括 Internet 上的计算机）”，这是默认选择，也可以选择“仅我的网络”（与你的计算机属于同一网络），还可以选择“自定义列表”（输入访问的是一台计算机、一组计算机或者是某几台计算机与某几组计算机的组合），如图 2-37 所示。

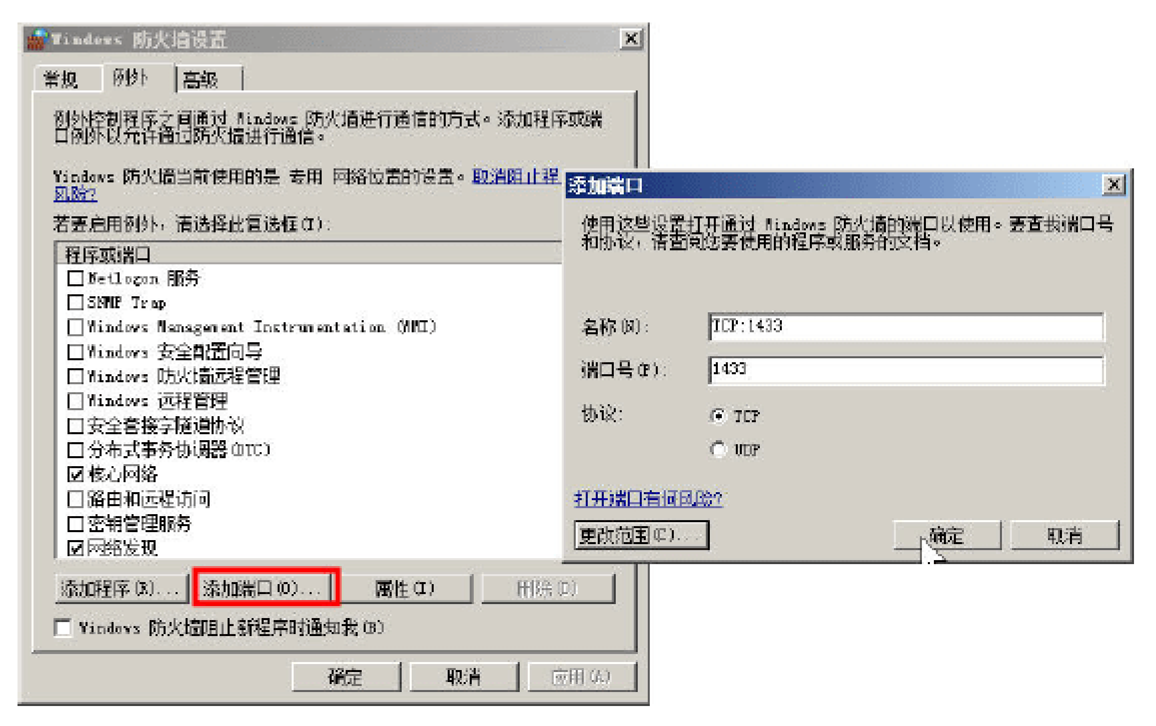


图 2-36　添加不存在的服务

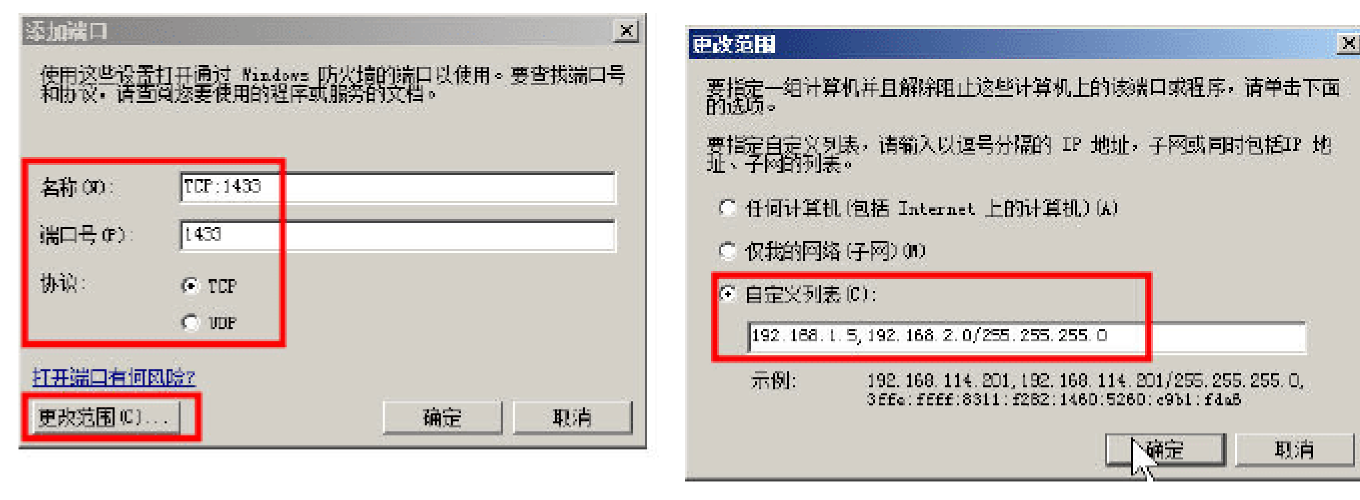


图 2-37　更改范围



说 明

在图 2-37 所示的“更改范围”对话框中，192.168.1.5 代表 192.168.1.5 这台计算机，192.168.2.0/255.255.255.0 表示 192.168.2.0～192.168.2.255 之间的所有计算机。另外，如果想确定某台计算机，也可以用子网掩码 255.255.255.255 来表示，如 192.168.1.5/255.255.255.255。

03 如果要解除对某种程序的封锁，可以在“Windows 防火墙设置→例外”中，单击“添加程序”按钮，在弹出的“添加程序”对话框中，选择当前系统中已经安装的程序，或者单击“浏览”按钮，浏览选择不在“程序”列表中的程序，如图 2-38 所示。也可以单击“更改范围”按钮，限制源网络。

04 如果该计算机有多块网卡，还可以在“高级”选项卡中，选择希望 Windows 防火墙所保护的网络，可以让“Windows 防火墙”只保护所选定的网络连接，如图 2-39 所示。

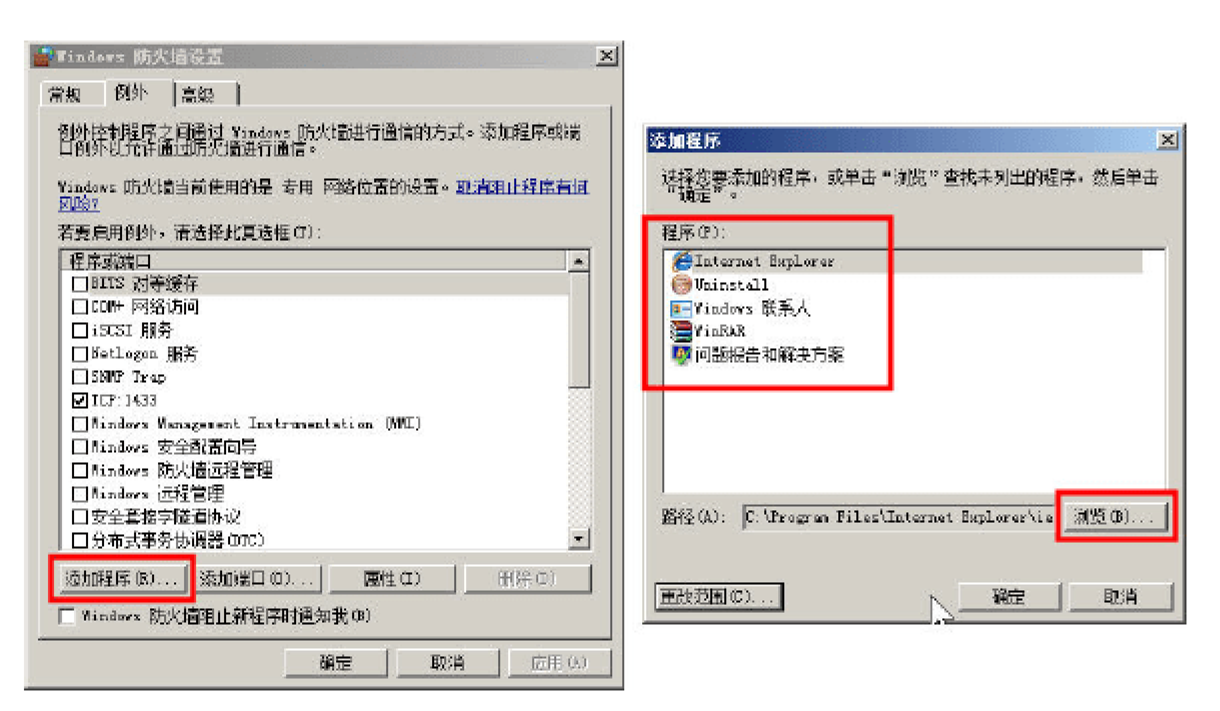


图 2-38　添加程序

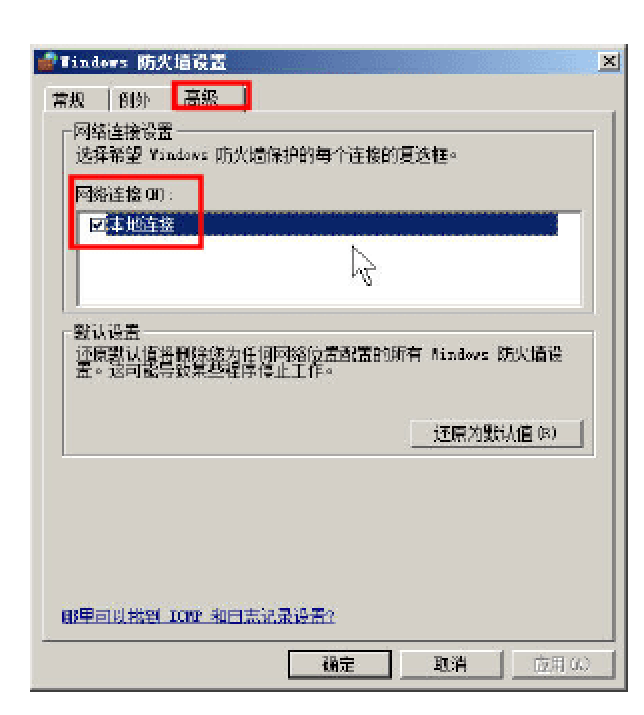


图 2-39　选择保护的网络

05 设置之后，单击“确定”按钮，完成设置。

2.4.4　高级安全 Windows 防火墙设置

在 Windows 防火墙中，只能对“入站规则”进行限制，如果想限制“出站规则”，或者需要对 Windows 防火墙的“入站规则”进行进一步设置，可以使用“高级安全 Windows 防火墙”功能。

01 在“开始→管理工具”中选择“高级安全 Windows 防火墙”，打开“高级安全 Windows 防火墙”程序，如图 2-40 所示。

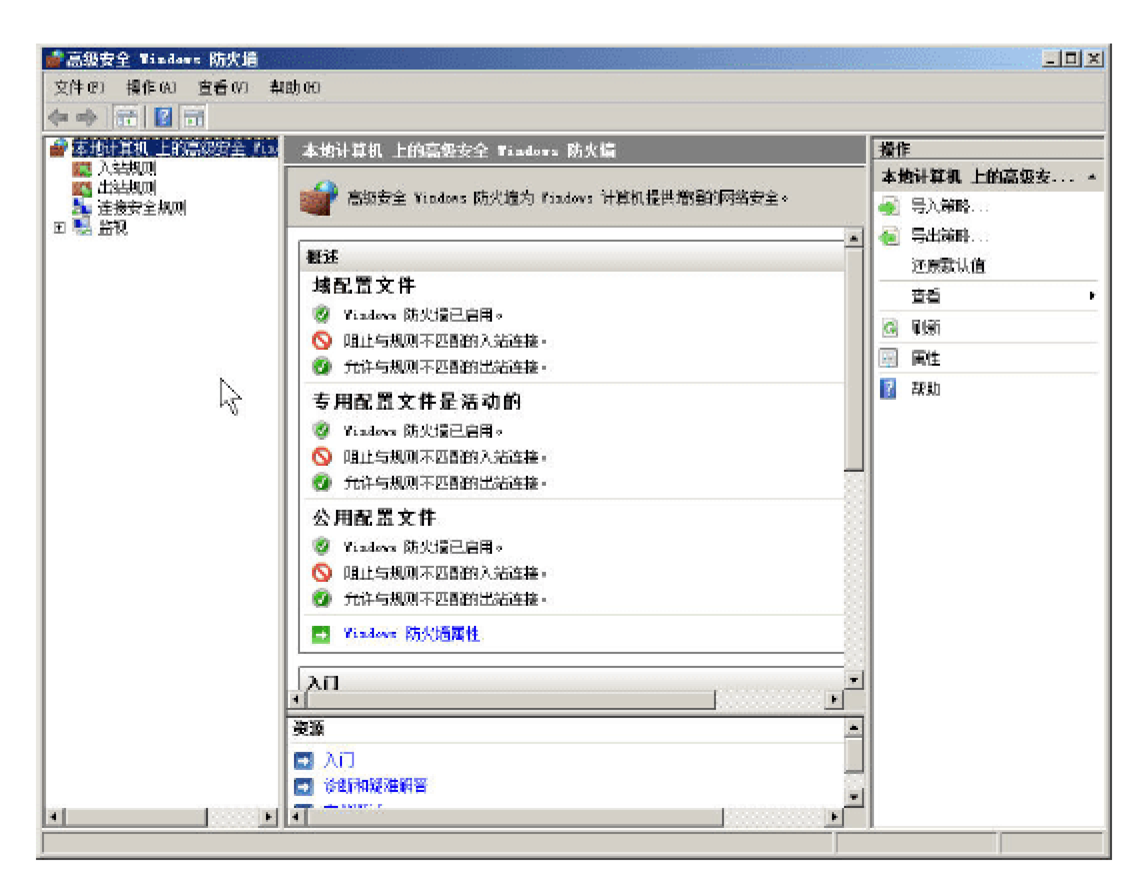


图 2-40　高级安全 Windows 防火墙

在“高级安全 Windows 防火墙”中，包括“入站规则”、“出站规则”、“连接安全规则”、“监视”等项，在工具栏上，单击“”可以显示或隐藏控制台树，单击“”显示或隐藏操作窗格。

02 在“入站规则”中，显示了系统中创建的一些规则，这些规则有的已经启用（规则前面是绿色的✓），有的处于禁用状态（规则前面是灰色的✓），可以右击选中一个规则，在弹出的快捷菜单中选择“启用规则（规则是禁用状态）”或“禁用规则（规则是启用状态）”。例如，如果允许网络中的计算机 ping 通本台计算机，可以启用“文件和打印机共享（回显请求-ICMPv4-In）”，如图 2-41 所示。

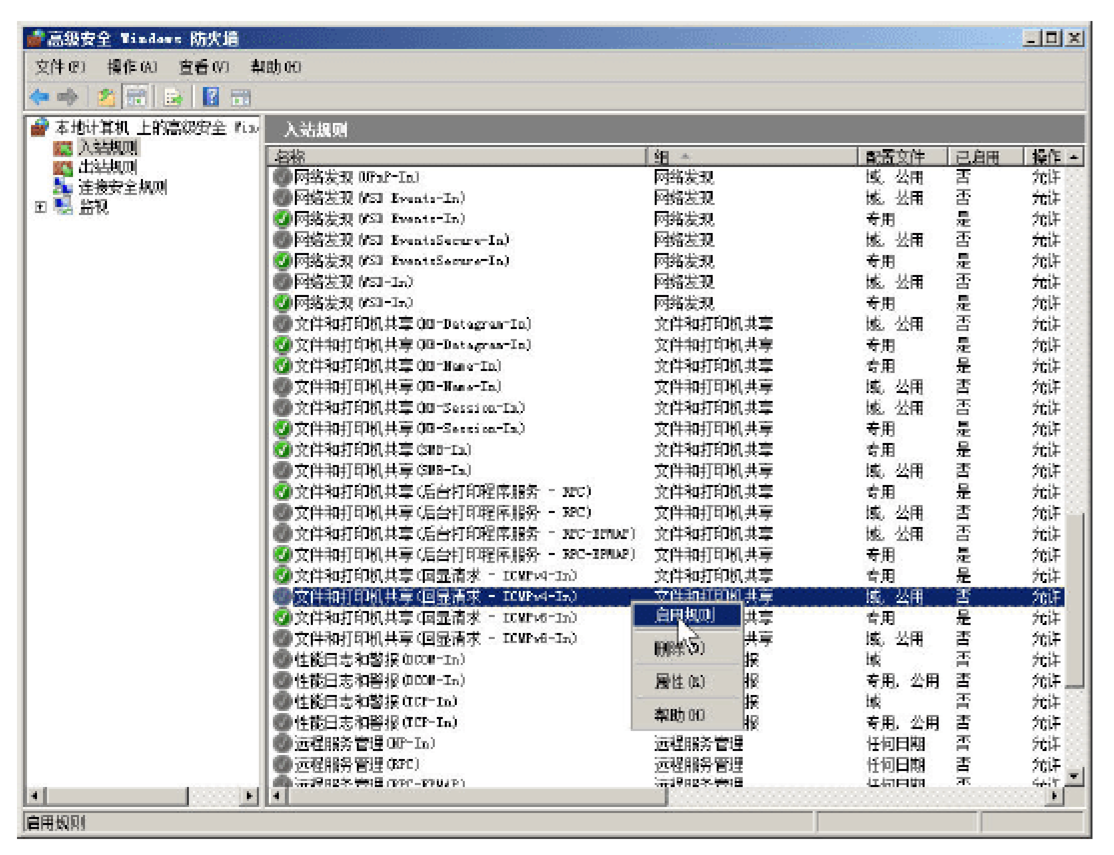


图 2-41　修改规则状态

03 在右击选中一个规则后，除了启用或禁用规则外，还可以删除该规则，也可以选中“属性”，查看该规则的详细信息，如图 2-42 所示。

04 如果要添加系统中不存在的规则，先选中“入站规则”或“出站规则”，在右侧的“操作”控制台中，单击“新规则”链接，在弹出的“新建入站（或出站）规则向导”中，根据向导进行操作即可，如图 2-43 所示。



图 2-42　规则属性

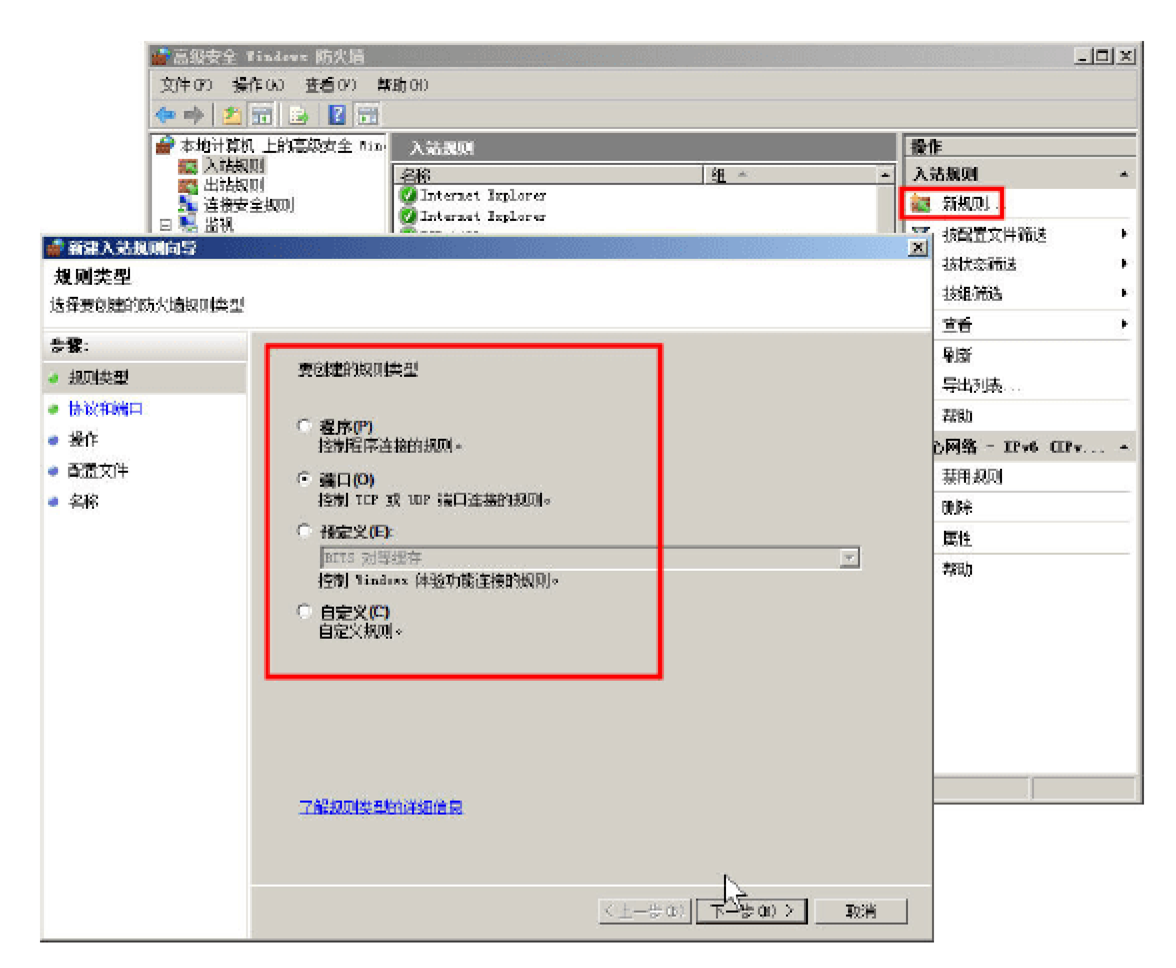


图 2-43　新建规则

05 在“监视→防火墙”中，显示了当前启用的防火墙规则，如图 2-44 所示。

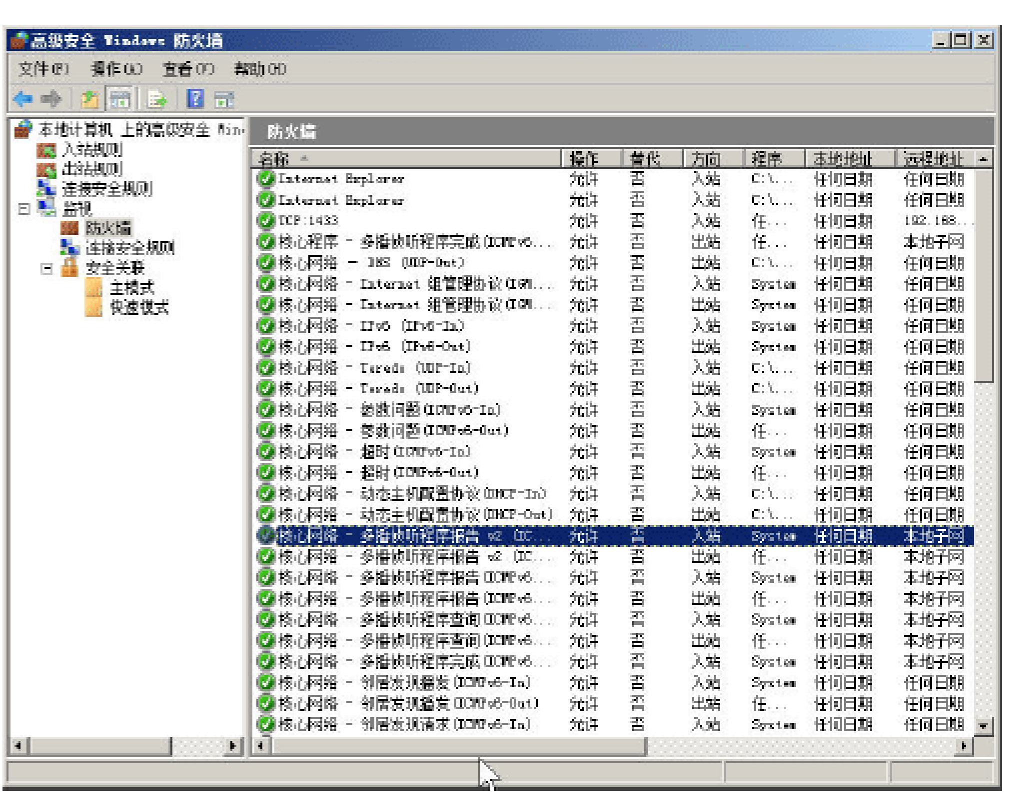


图 2-44　启用的防火墙规则

2.5　系统属性设置与修改

在“系统”属性中，包括“设备管理器”、“远程设置”、“高级系统设置”三部分内容，可以修改计算机的名称、设置虚拟内存，配置远程桌面、文件、环境等内容。

2.5.1　系统任务

从“开始”菜单右击“计算机”，在弹出的快捷菜单中选择“属性”选项（如图 2-45 所示），将会打开“系统”窗口，如图 2-46 所示。

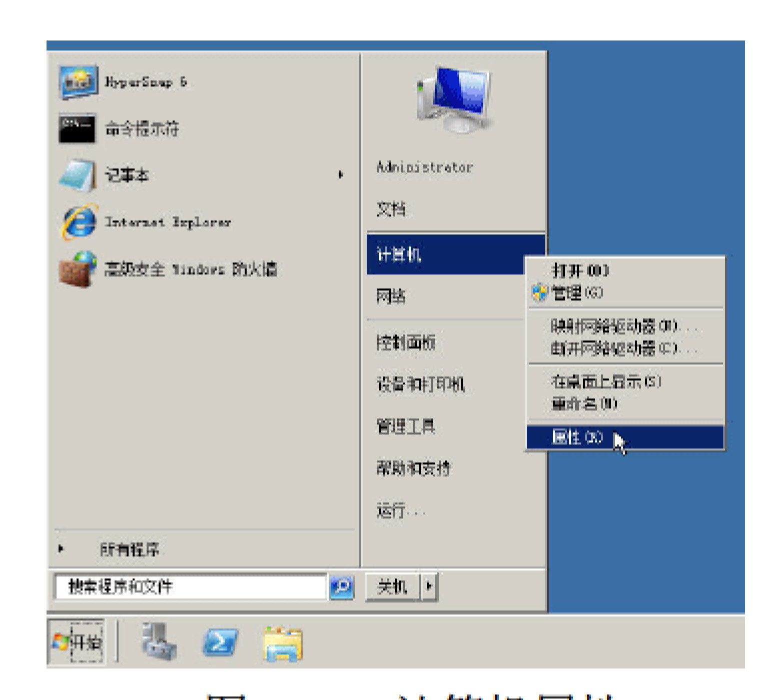


图 2-45　计算机属性



图 2-46　系统任务

2.5.2　设备管理器

在图 2-46 左侧窗体中，单击“设备管理器”链接（或者在图 2-45 所示菜单中右击“计算机”，在弹出的快捷菜单中选择“管理”，打开“服务器管理器”窗口，在“诊断”中选择“设备管理器”），打开“设备管理器”控制台，如图 2-47 所示。

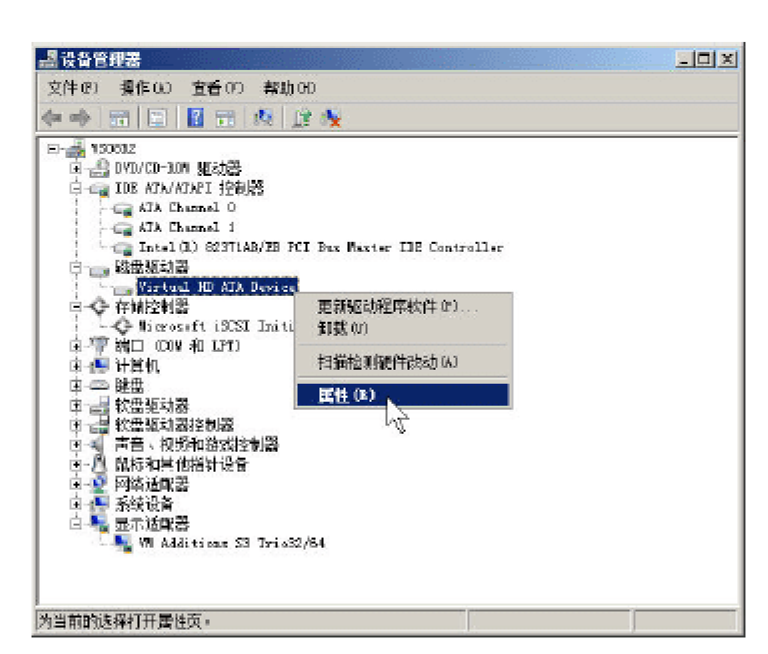


图 2-47　设备管理器

在“设备管理器”中，可以实现下列功能：

- 为没有安装驱动程序的设备（通常设备名称前面有黄色的感叹号）安装驱动程序（需要有适合当前操作系统的该设备的驱动程序文件）。
- 卸载不再需要的设备。
- 更新设备驱动程序，或者返回上一版本驱动程序。
- 对设备进行进一步的设置。

例如，在图 2-47 所示的窗口中，右击“磁盘驱动器→Virtual HD ATA Device”，在弹出的快捷菜单中选择“属性”选项，打开该虚拟磁盘的属性页，在“策略”选项卡中，选择“启用磁盘上的写入缓存”与“启用高级性能”复选框，如图 2-48 所示。



说 明

如果是 USB 等外接存储设备，一般选择“为快速删除而优化”，这样可以在不使用设备时，随时拔出该设备。

在“驱动程序”选项卡中，可以查看驱动程序的详细信息，也可以“更新驱动程序”（需要有最新的驱动程序文件），如果该设备安装了多个版本的驱动程序，可以单击“回滚驱动程序”按钮，选择上一个驱动程序，如图 2-49 所示。

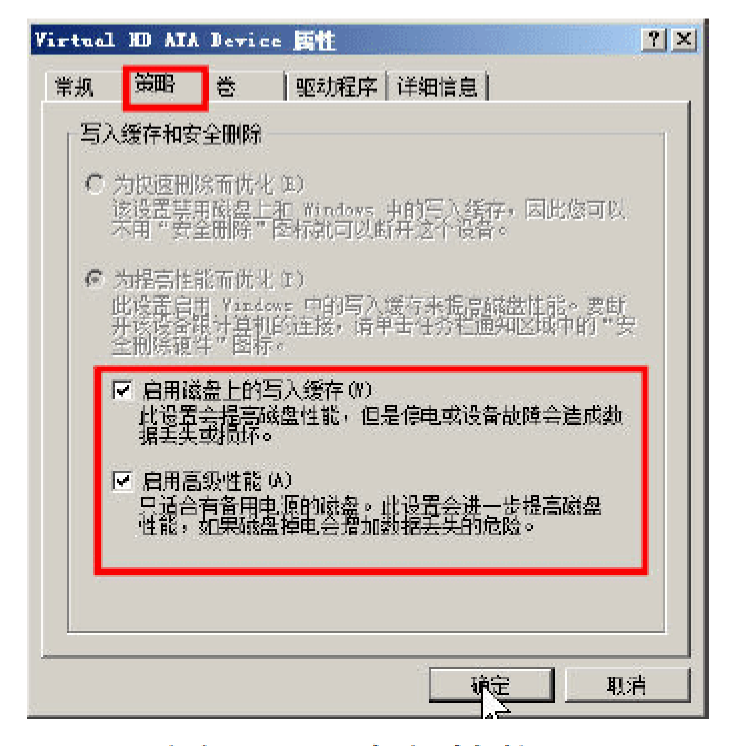


图 2-48　高级性能

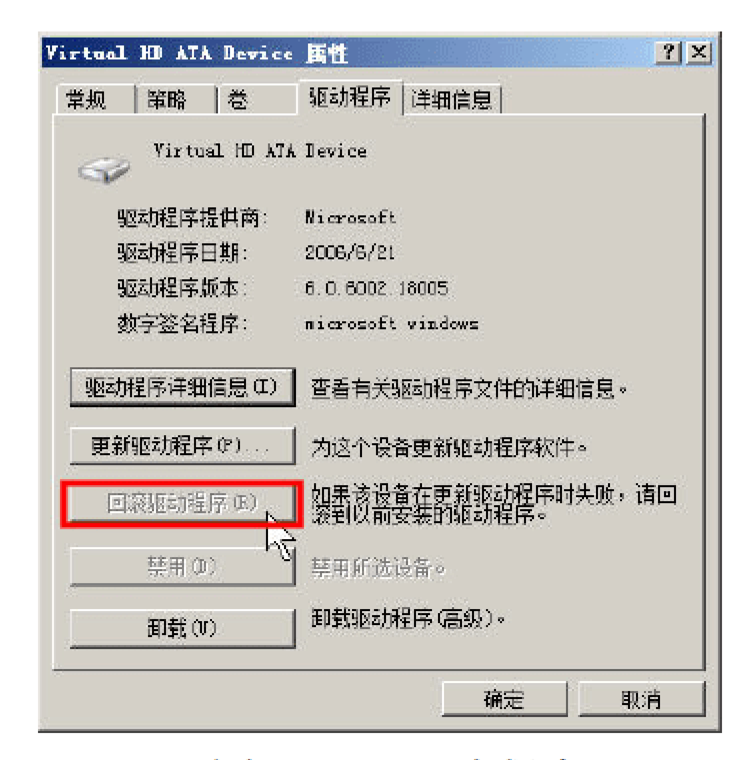


图 2-49　驱动程序

2.5.3　远程设置

在图 2-46 所示的窗口中单击“远程设置”链接，打开“系统属性→远程”对话框，在该对话框中，可以设置“远程协助”与“远程桌面”，对于 Windows Server 2008 等服务器操作系统来说，“远程桌面”是一个非常有用的功能，启用该功能后，可以在网络中任意一台装有 Windows 操作系统的计算机上，使用“远程桌面客户端”连接到这台服务器。

对于 Windows Server 2008 来说，如果想让低版本的操作系统（Windows XP、Windows Server 2003）的远程桌面客户端连接到这台计算机，可以选择“允许运行任意版本远程桌面的计算机连接（较不安全）”选项；如果选中“只允许运行带网络级身份验证的远程桌面的计算机连接（更安全）”选项，则至少需要 Windows Vista（及其以后版本如 Windows 7、Windows Server 2008）操作系统的计算机，才能连接到该计算机。可以根据情况，选择是否开启远程桌面、开启何种版本的远程桌面，如图 2-50 所示。

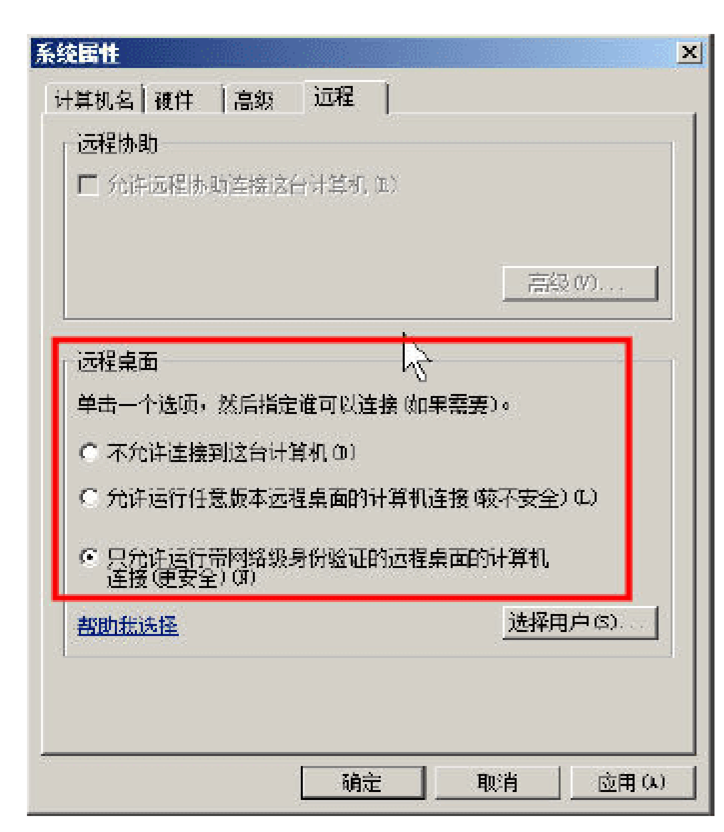


图 2-50　远程桌面

2.5.4 高级系统设置

在“系统属性”对话框中，打开“高级”选项卡，进入“高级系统设置”页面，如图 2-51 所示，在此可以调整视觉效果、虚拟内存、用户配置文件、启动和故障恢复、环境变量等。

01 在“性能”选项组中，单击“设置”按钮，进入“性能选项”对话框，在“视觉效果”

选项卡中，选择想在此计算机上使用的 Windows 外观和性能设置。对于服务器操作系统来说，获得最好的性能是首选，所以，可以选中“调整为最佳性能”，如图 2-52 所示。如果是 Windows 7 操作系统，则可以选择“调整为最佳外观”，或者选择“让 Windows 选择计算机的最佳设置”。也可以选择“自定义”，并在“自定义”列表中选择需要的每一个效果。

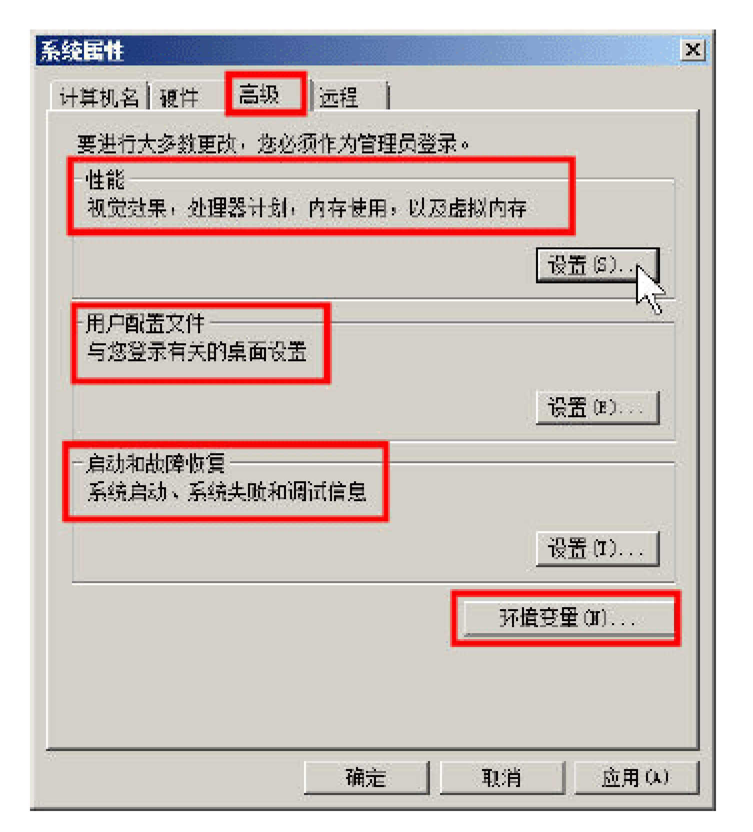


图 2-51　高级系统设置

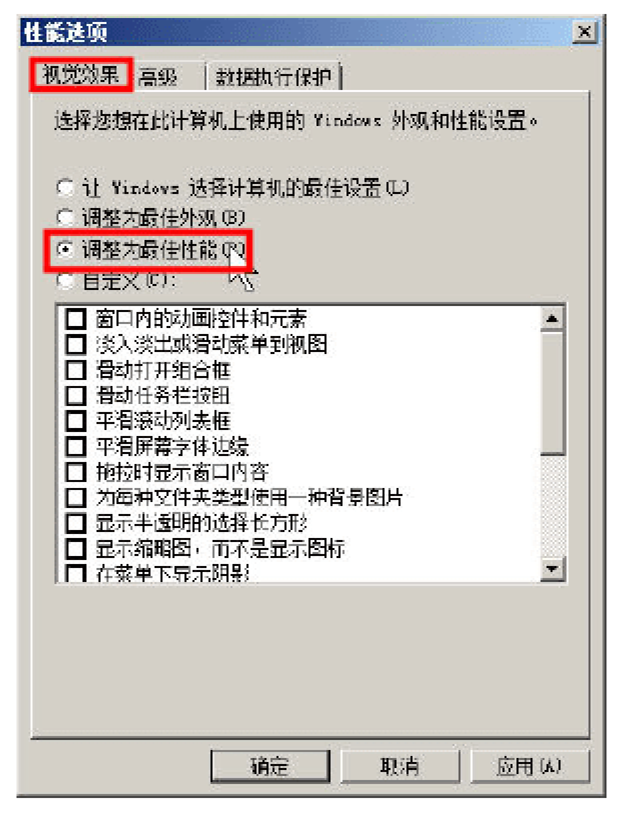


图 2-52　视觉效果

02 在“高级”选项卡中，在“处理器计划”选项组中，选择分配处理器资源是为“程序”还是“后台服务”进行优化。在“虚拟内存”选项组中单击“更改”按钮，打开“虚拟内存”对话框，默认情况是“自动管理所有驱动器的分页文件大小”（系统自动管理）。如果想自己设置，可以取消这一项设置，并且选中当前系统的每个分区，进行设置，这可以在“自定义大小”、“系统管理的大小”、“无分布文件”三者之间进行选择，如图 2-53 所示。

03 在图 2-51 所示的对话框中，在“用户配置文件”选项组中，单击“设置”按钮，打开“用户配置文件”对话框，在此可以更改配置文件类型（漫游配置文件、本地配置文件），“删除”不使用的配置文件，或者将现有的配置文件复制到其他用户，如图 2-54 所示。

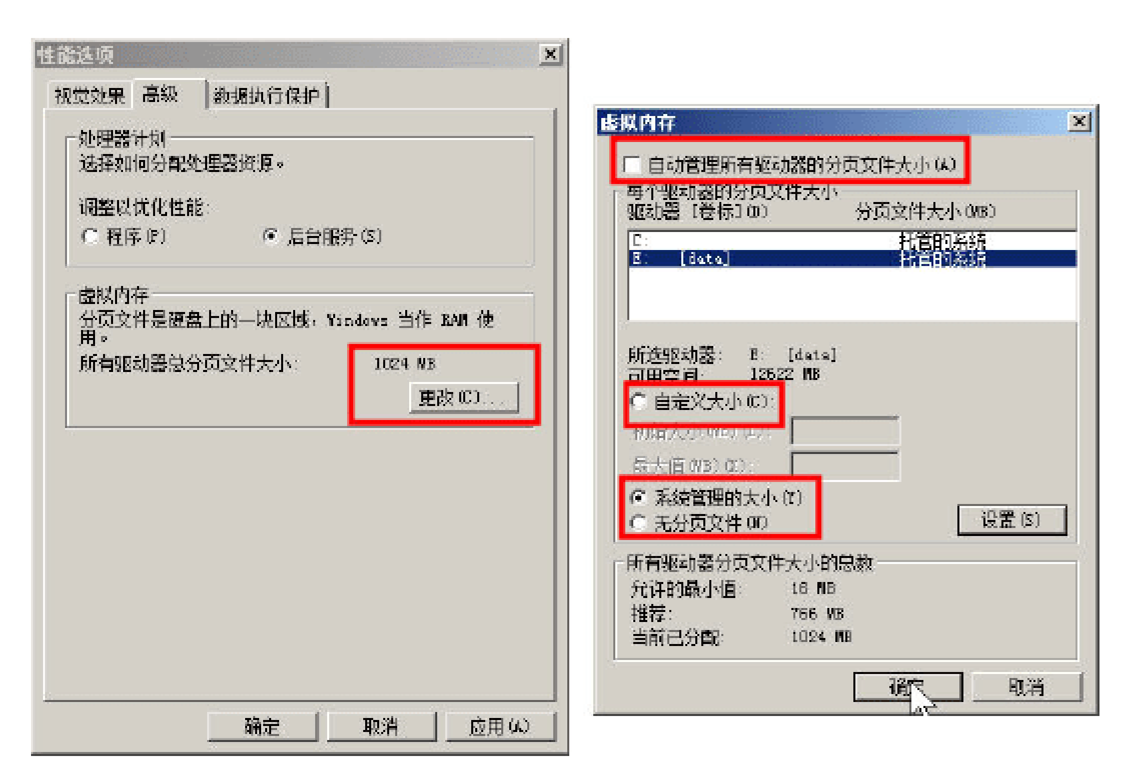


图 2-53　处理器计划与虚拟内存

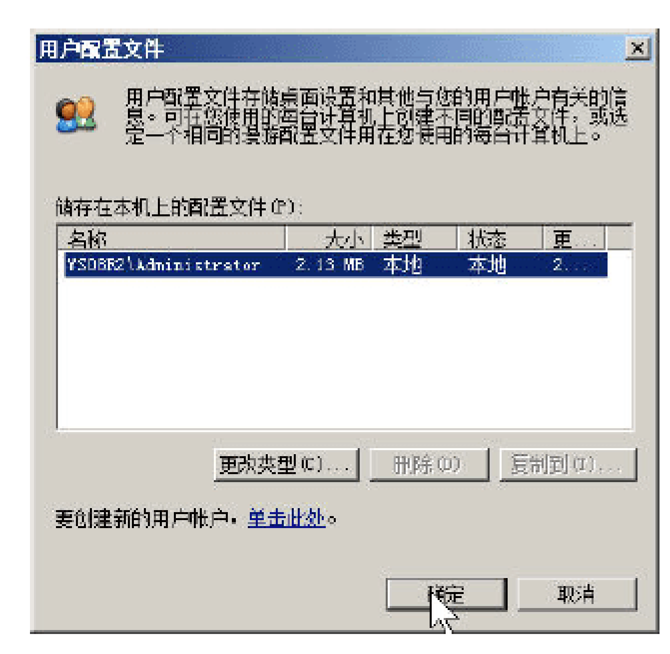


图 2-54　用户配置文件

04 在图 2-51 所示的对话框中，在“启动和故障恢复”选项组中，单击“设置”按钮，打开“启动和故障恢复”对话框，在此可以设置“系统启动”选项，如果有多个系统，可以选择“默认启动”的操作系统，或者选中“显示操作系统列表的时间”、“在需要时显示恢复选项的时间”复选框，在“系统失败”选项组中，取消“自动重新启动”选项，在“写入调试信息”列表中选择“无”，

如图 2-55 所示。

05 在图 2-51 所示的对话框中，单击“环境变量”按钮，打开“环境变量”对话框，在此可以设置用户或系统的“变量”，如图 2-56 所示。

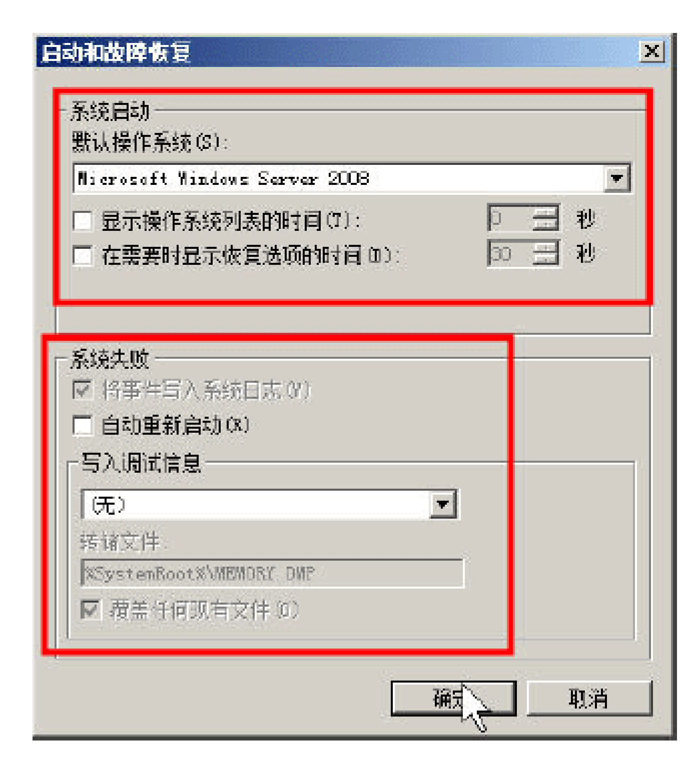


图 2-55　启动和故障恢复

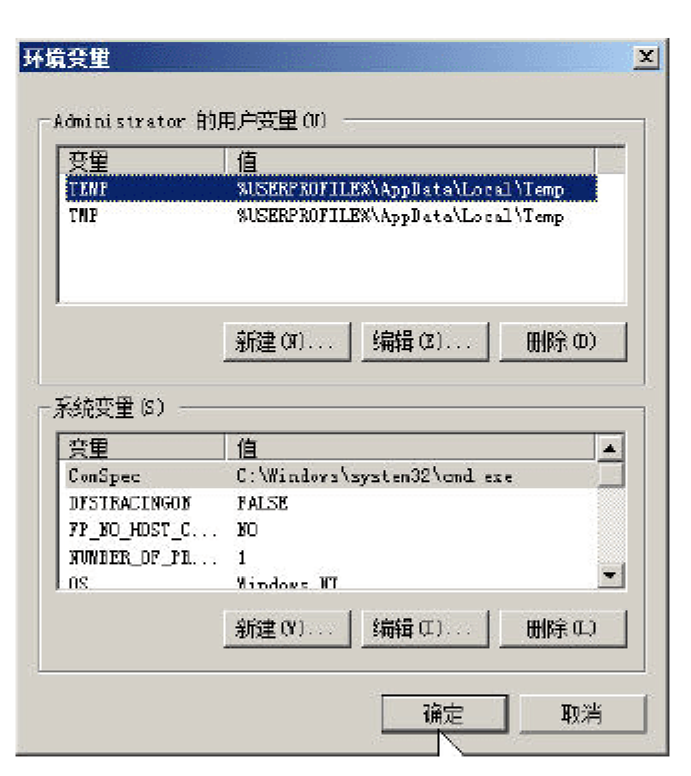


图 2-56　环境变量

2.5.5　Windows Update 驱动程序设置

在“系统属性”对话框中，打开“硬件”选项卡，可以看到“设备管理器”与“Windows Update 驱动程序设置”设置项，单击“Windows Update 驱动程序设置”按钮，弹出“Windows Update 驱动程序设置”对话框。当系统安装（或连接）一个新设备时，如果当前系统没有安装该设备的驱动程序，想让 Windows Update 查找匹配的驱动程序，推荐选择“自动检查驱动程序”，系统会自动连接到网络查找驱动程序并下载、安装，如图 2-57 所示。

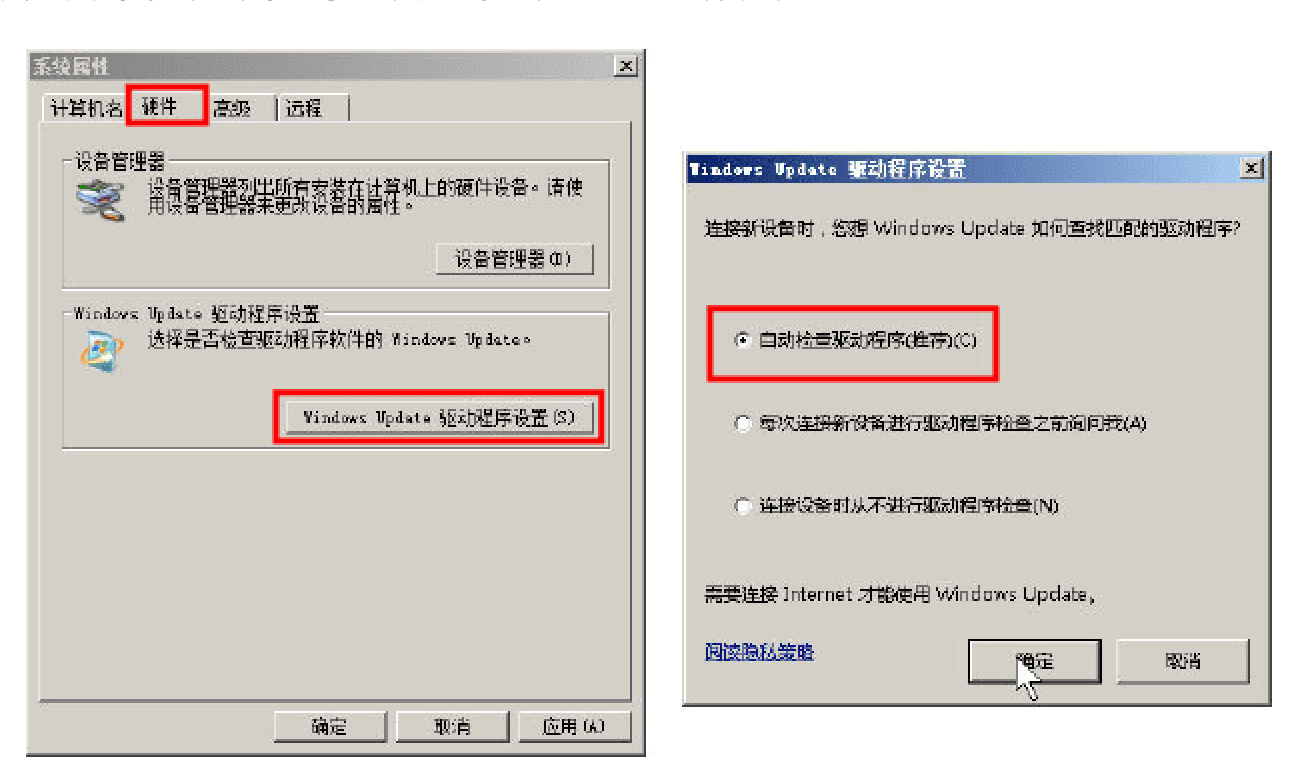


图 2-57　Windows Update 驱动程序设置


说　明

该项功能在 Windows Server 2003 中已经提供，但在以前的版本中，即使是通过 Windows Update 也经常不能检查到合适的驱动程序。从 Windows Vista 开始，Microsoft 改进了这项功能，提高了通过 Windows Update 安装程序的成功率。

2.5.6　计算机名

在“系统属性”对话框中，打开“计算机名”选项卡，可以修改计算机的名称、是否将计算机加入到域或工作组，或者修改“计算机描述”信息，如图 2-58 所示。在系统属性设置完成之后，单击“确定”按钮退出，如果修改了虚拟内存或计算机名称，系统会提示重新启动，如图 2-59 所示。

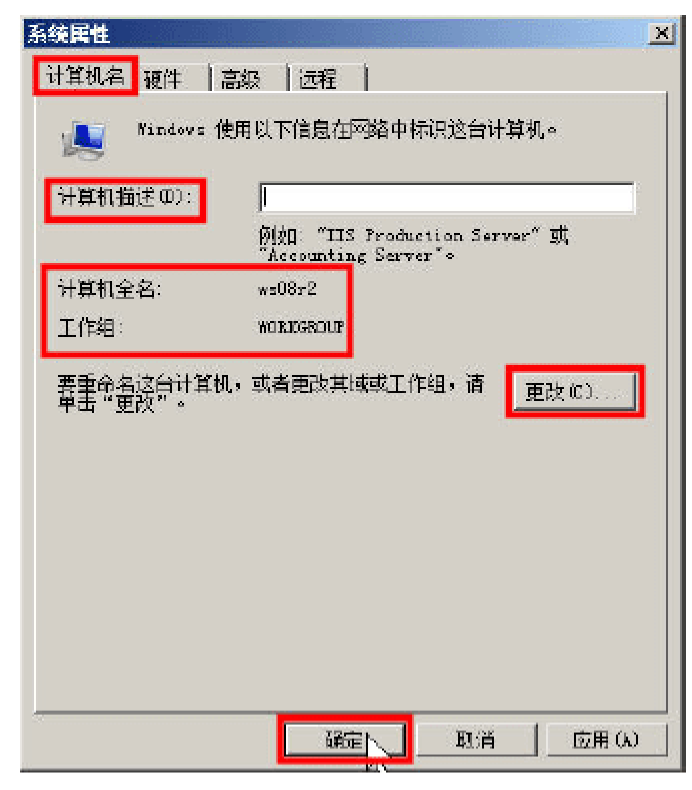


图 2-58　计算机名

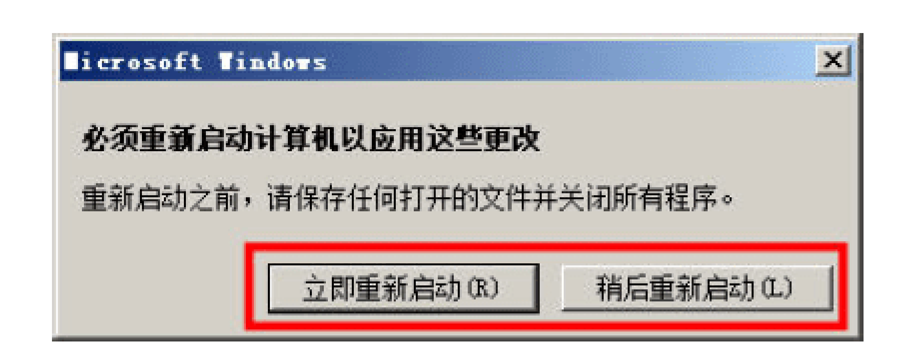
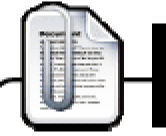


图 2-59　提示重新启动计算机

2.6　计算机管理

如果 2-60 所示，“计算机管理”包括“系统工具”、“存储”、“服务和应用程序”三部分。其中“系统工具”包括“任务计划程序”、“事件查看器”、“共享文件夹”、“本地用户和组”、“可靠性和性能”、“设备管理器”等组件（或功能）；“存储”管理主要是指“磁盘管理”；“服务和应用程序”包括“路由和远程访问”、“服务”、“WMI 控制”三部分内容。“计算机管理”中组件比较多，我们将介绍常用的部分。



说　明

“从开始”菜单选择“管理工具→计算机管理”，可以进入“计算机管理”控制台，如图 2-60 所示。

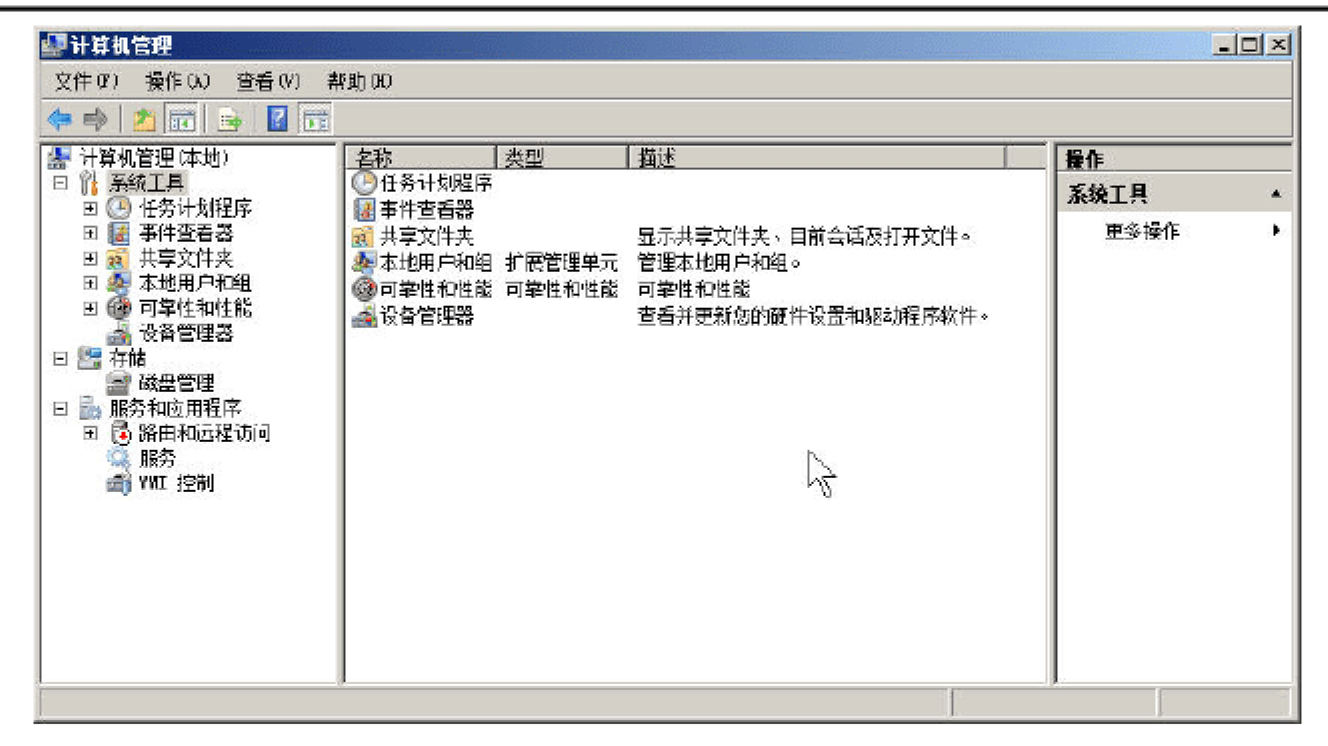


图 2-60　计算机管理

2.6.1　任务计划程序

在“任务计划程序”中，可以创建（或管理）计算机在指定的时间自动执行的常见任务。单击“系统工具→任务计划程序，在窗体右侧的“操作”列表中选择“创建基本任务”或“创建任务”都可以创建任务计划程序。这两者的区别是：“创建基本任务”是采用向导的方式创建任务计划程序，而“创建任务”则是采用对话框的方式创建任务计划程序，两者创建的任务程序都可以完成相同的任务及操作。在本例中，使用后者来介绍。

01 用鼠标右击“任务计划程序”，在弹出的快捷菜单中选择“创建任务”，如图 2-61 所示。

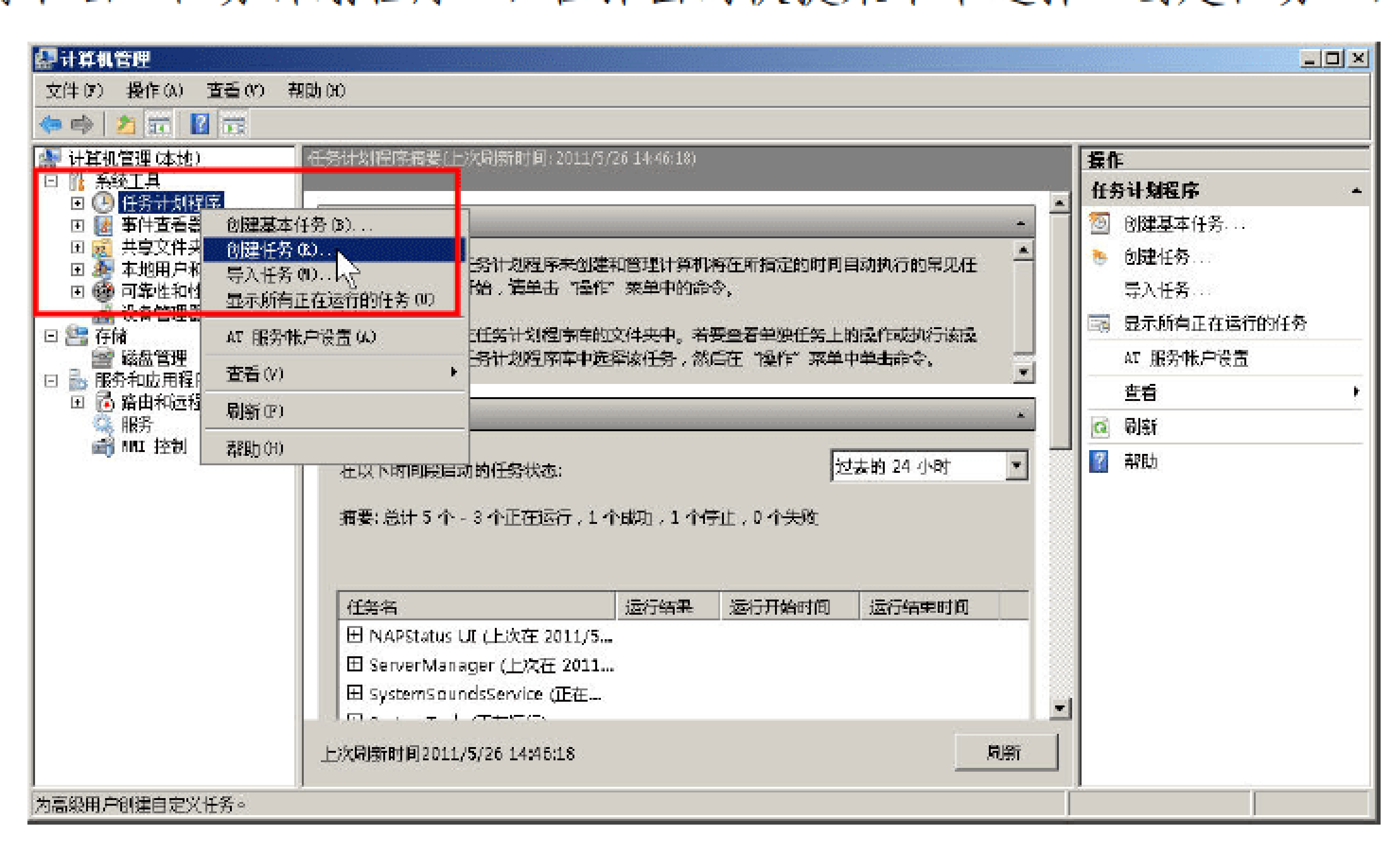


图 2-61　创建任务

02 在“常规”选项卡中，在“姓名”文本框中，输入创建的任务的名称，在“描述”文本框中，输入当前新建任务的描述信息。在“创建者”后面列出了系统当前的登录用户（也即任务的“创建者”），如果要更改任务的运行账户，可以单击“更改用户或组”按钮进行设置。在“安全选项”中，如果选择“只在用户登录时运行”，则当前的操作系统只有在登录进入系统之后才能运行该任务；如果选择“不管用户是否登录都要运行”，则不管当前系统是否登录，都会运行，如图 2-62 所示。

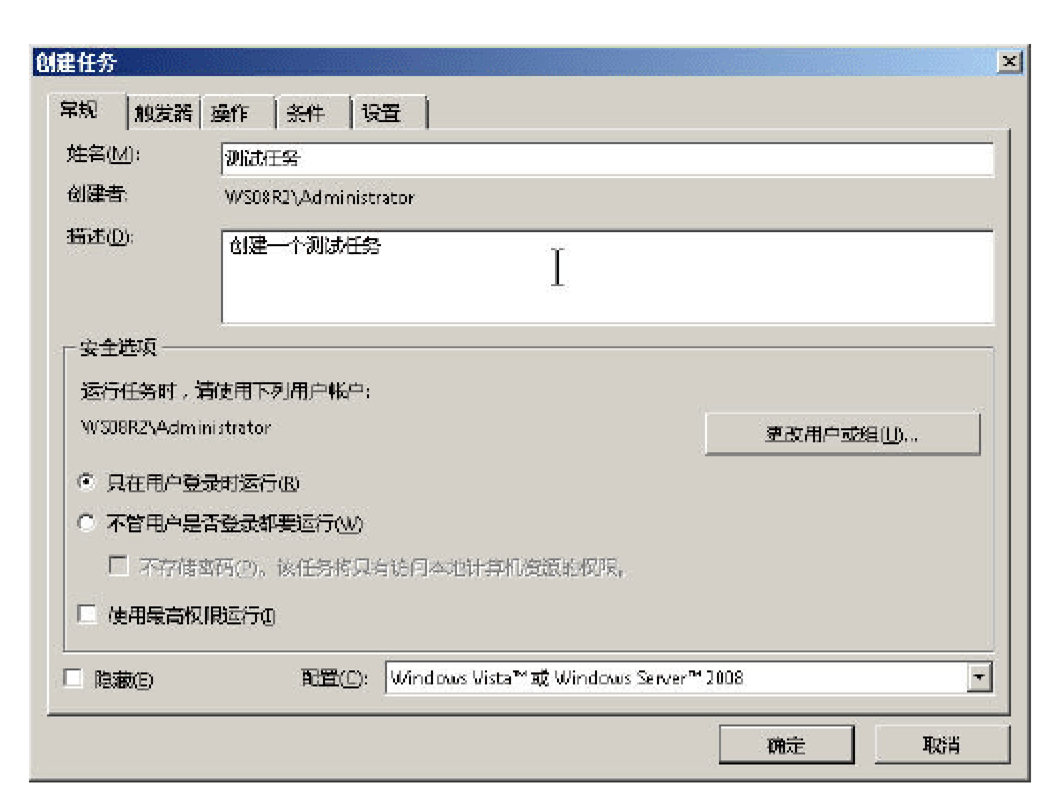


图 2-62　常规

03 在“触发器”选项卡中，单击“新建”按钮，选择触发该任务的条件。“开始任务”的

条件可以是“制定计划时”、“登录时”、“启动时”、“空闲状态”、“发生事件时”、“创建/修改任务时”、“当连接到用户会话时”、“当从用户会话断开连接时”、“工作站锁定时”、“工作站解锁时”，如图 2-63 所示。

在选定“开始任务”的时刻后，在“设置”选项组中，选择任务的执行频率（可以是一次、每天、每周、每月，或者指定的日期和时间），在“高级设置”选项组中，设置任务的延迟时间、重复任务间隔、停止运行条件、过期日期等，如图 2-64 所示。

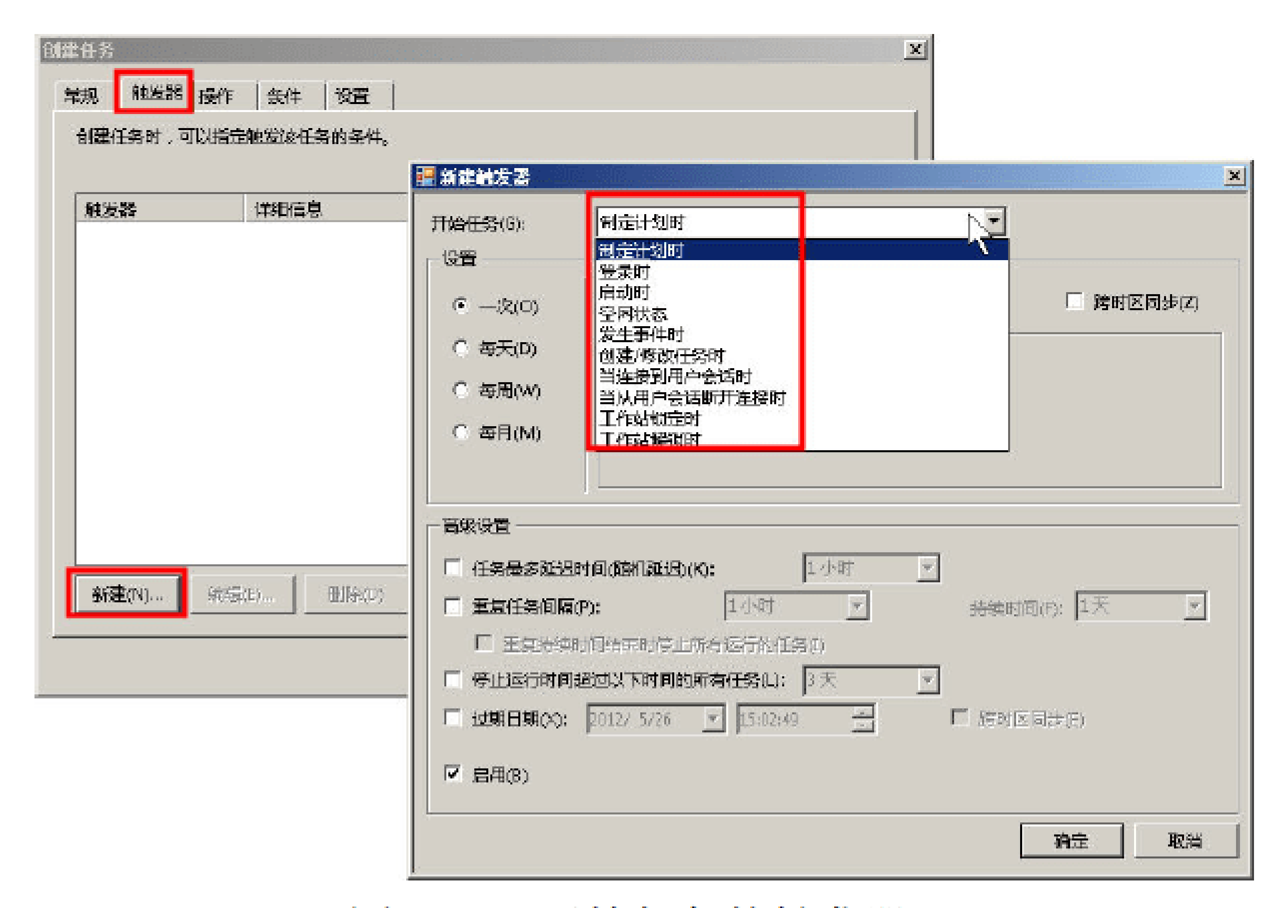


图 2-63　开始任务的触发器

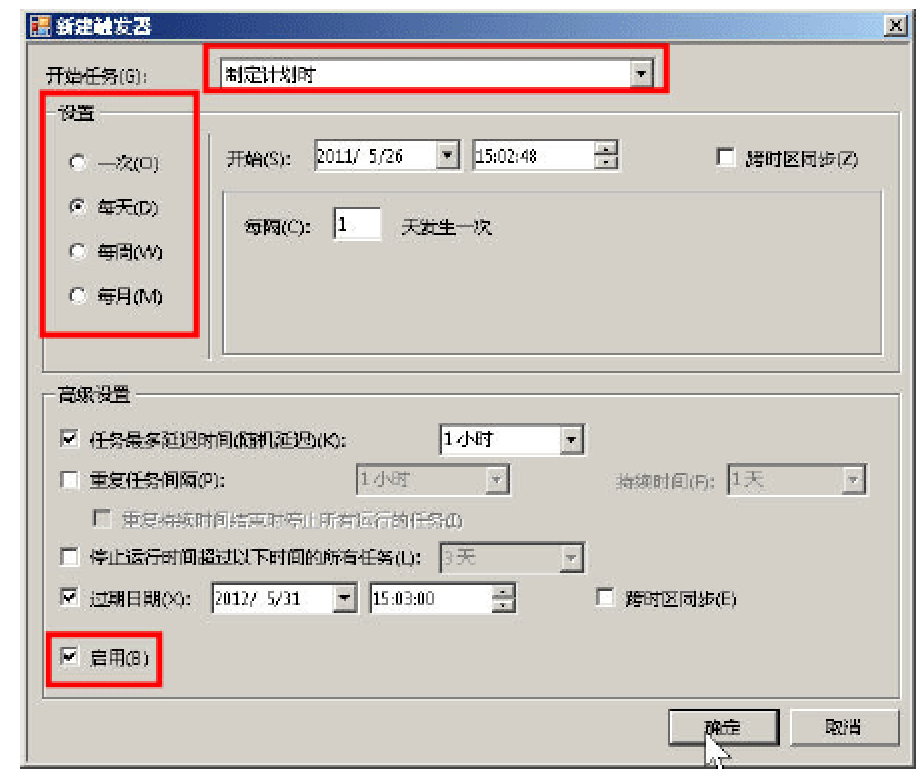


图 2-64　触发器

如果当前创建的任务计划暂时不起作用，可以取消“启用”选项，这样任务将不会生效。

04 在“操作”选项卡中，选择启动任务时要执行的操作，这可以是“启动程序”（启动一个程序或批处理）、“发送电子邮件”（向指定的邮箱发送电子邮件）或“显示消息”（在当前计算机屏幕上显示一个消息），如图 2-65 所示。

05 在“条件”选项卡中，指定用于与触发器一起判断是否应该运行该任务的条件，如果这里指定的任务不为“真”，则该任务不会运行。这些条件可以是“仅当计算机空闲时间超过下列值时才启动此任务”、“只有在计算机使用交流电源时才启动此任务”、“只有在以下网络连接可用时才启动”等，如图 2-66 所示。这些可根据情况进行选择。

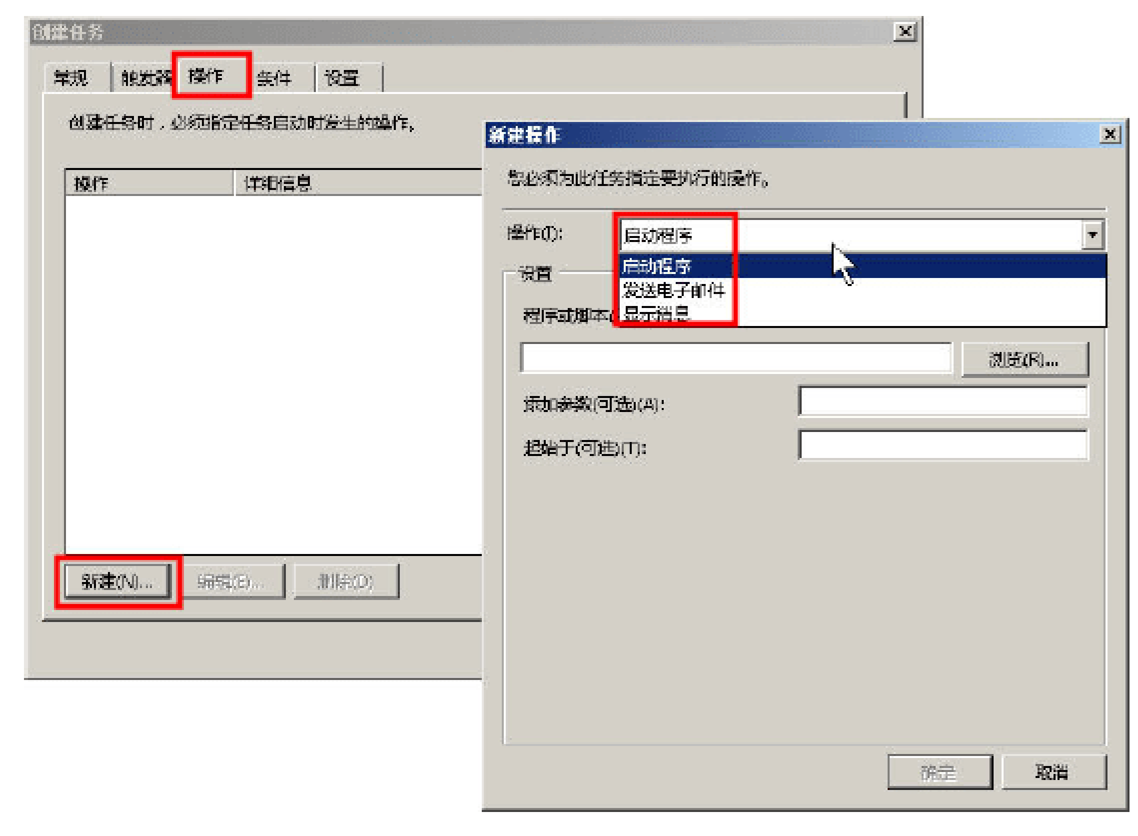


图 2-65　任务操作

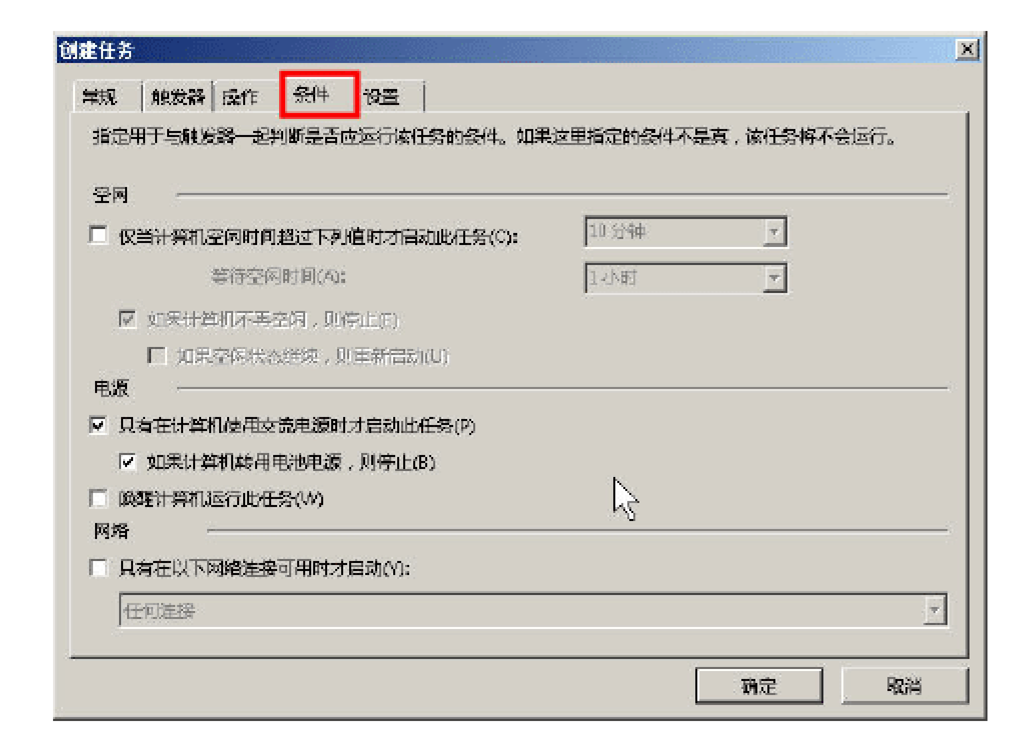


图 2-66　条件

06 在“设置”选项卡，设置影响任务的其他设置，这包括“允许按需运行任务”、“如果过了计划开始操作，立即启动任务”、“如果任务失败，按以下频率重新启动”、“如果任务运行时间超过以下时间，停止任务”、“如果请求后任务还在运行，强行将其停止”、“如果任务没有计划再次运行，则在此之后删除该任务”等，如图 2-67 所示。

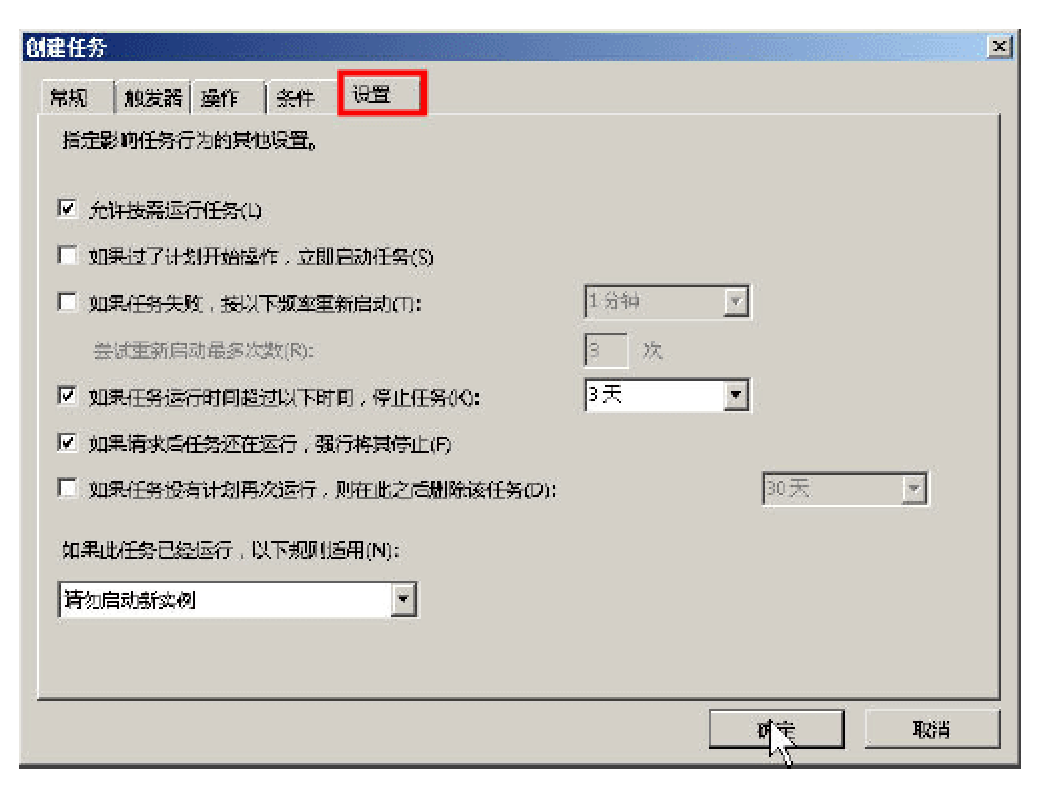


图 2-67　设置

在图 2-67 所示的对话框中，可以选中相应的设置，并设置相应的时间或次数。设置好任务之后，单击“确定”按钮。

创建好任务之后，单击“系统工具→任务计划程序→任务计划程序库”，可以看到创建的任务，用鼠标右键单击，可以选择“运行→直接运行任务”、“结束→结束运行的任务”、“禁用→停用任务”、“导出→导出任务设置”、“属性→打开任务属性对话框，修改或配置任务”、“删除→删除任务”，如图 2-68 所示。

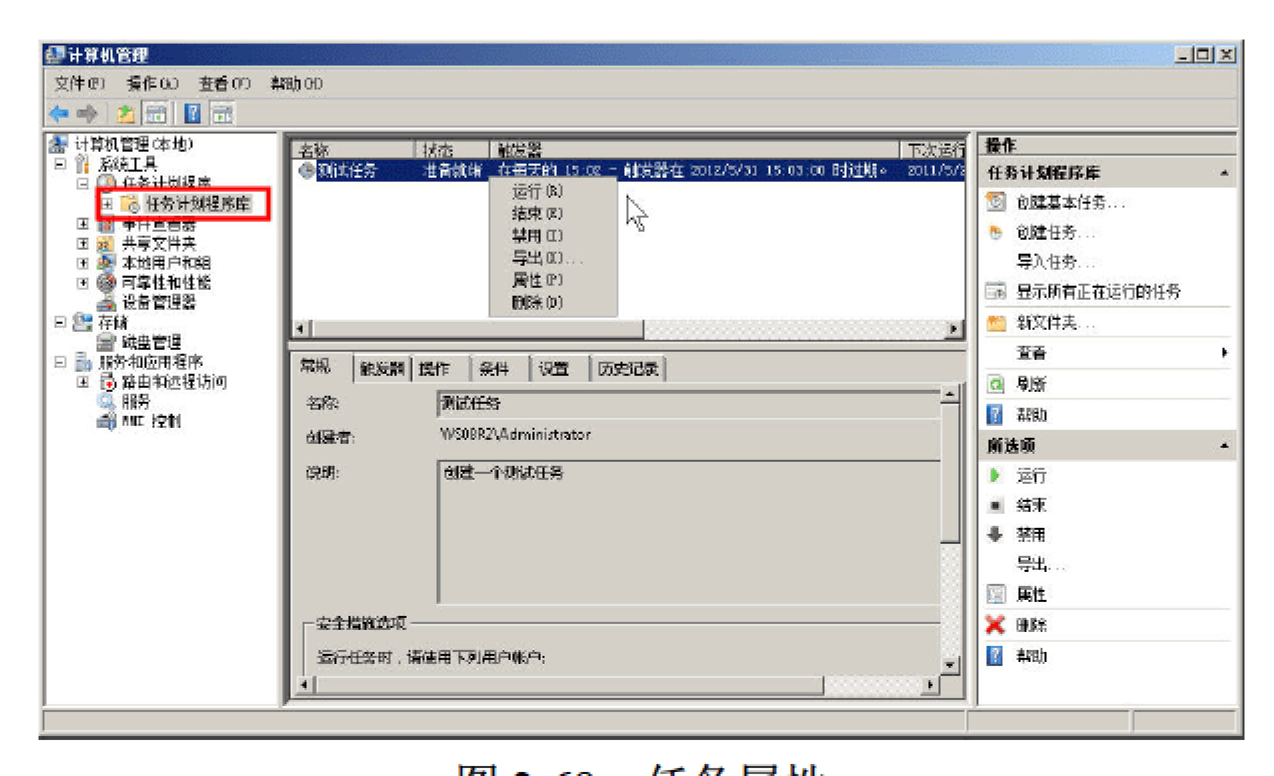


图 2-68　任务属性

2.6.2　配置操作系统的自动登录

在图 2-62 所示的对话框中，如果选中“只在用户登录时运行”，则该任务需要在系统登录之后才能运行。如果服务器重新启动，是不能自动登录进入系统的，此时该任务将不会运行。如果让服务器重新启动之后，自动以管理员账户（Administrator）登录，则可以按照如下操作进行配置。

01 打开“运行”对话框，输入“control userpasswords2”，如图 2-69 所示。

02 在弹出的“用户账户”对话框中，取消“要使用本地，用户必须输入用户名和密码”的选项，在弹出的“自动登录”对话框中，输入管理员账户的密码，然后单击“确定”按钮，完成设置，如图 2-70 所示。

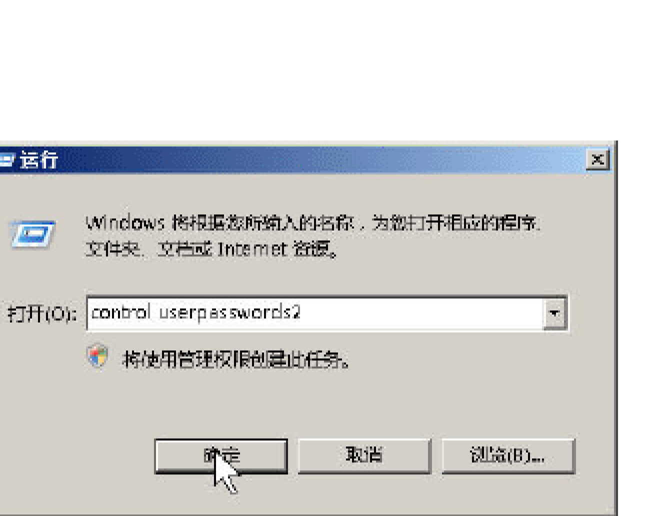
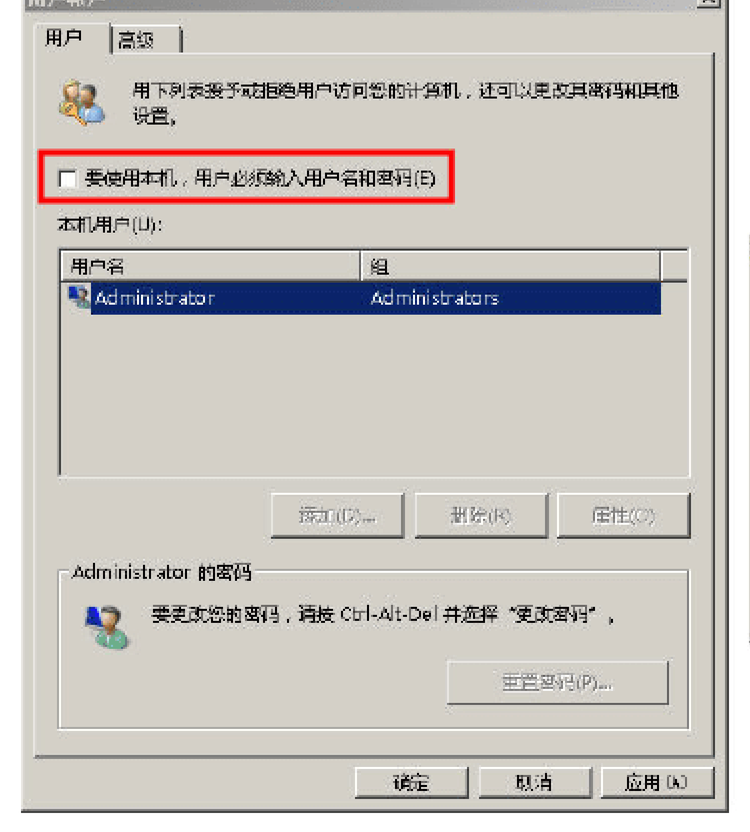


图 2-69　运行命令



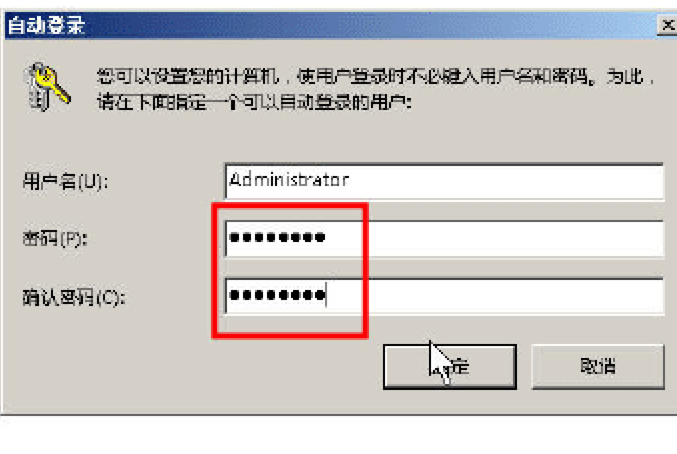


图 2-70　自动登录设置

经过这样设置，可以自动登录系统。

2.6.3　事件查看器

“事件查看器”是一个 Microsoft 管理控制台（MMC）的管理单元，可以用于浏览和管理事件日志。当系统出现问题时，除了按照自己的习惯、方式分析、判断发生的原因以解决之外，还可以通过“事件查看器”查看系统的运行状态，以及在出现问题时，查看系统提供的解决方案。

在“计算机管理→系统工具→事件查看器”中，可以查看“应用程序”、“安全”、“Setup”、“系统”、“转发的事件”等 Windows 日志，还可以查看某些应用程序和服务日志。如果想要查看某个事件的详细记录，可以双击一个日志进行查看，如图 2-71 所示。如果要查看系统提供的解决方法（或者事件的产生原因）等，可以单击“事件日志联机帮助”链接，系统会使用浏览器连接到 Microsoft 公司专门为“事件查看器”创建的网站，打开该事件对应解决方法的记录。

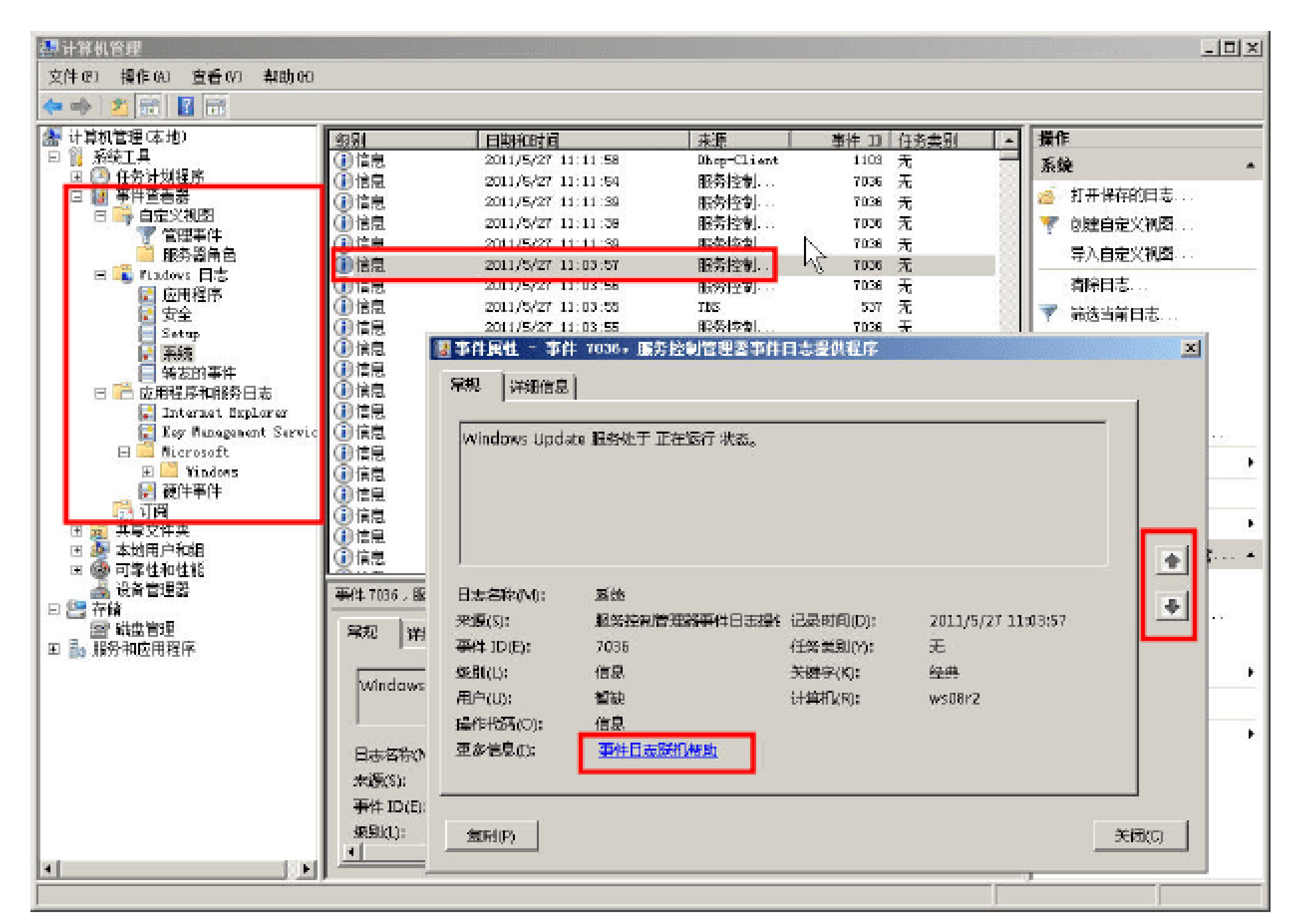


图 2-71　事件查看器

在图 2-71 所示的对话框中，查看完一个事件之后，可以通过单击“↑”、“↓”按钮，浏览查看上一个、下一个事件的详细信息。也可以单击“关闭”按钮，关闭选中的事件。

2.6.4　共享文件夹

可以使用“共享文件夹”管理单元集中管理计算机上的文件共享。共享文件夹允许创建文件共享和设置权限，查看和管理打开的文件以及连接到计算机上文件共享的用户。

01 在“共享文件夹→共享”选项中，可以创建共享、删除共享，或者选中一个共享，修改共享权限，如图 2-72 所示。

02 在“共享文件夹→会话”选项中，可以查看是否有用户连接到该计算机，如果有用户连接到该计算机，会显示客户端计算机的名称、连接的用户名、打开的文件数量、连接时间、空闲时间等，可以用鼠标右击选中一个打开的文件，关闭打开的连接，如图 2-73 所示。

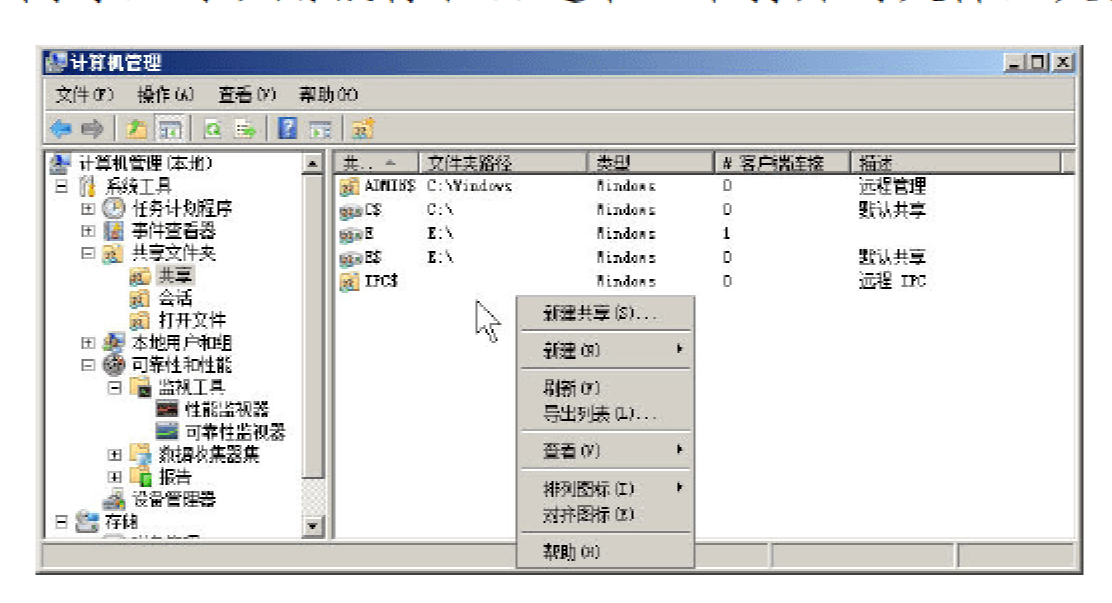


图 2-72　共享

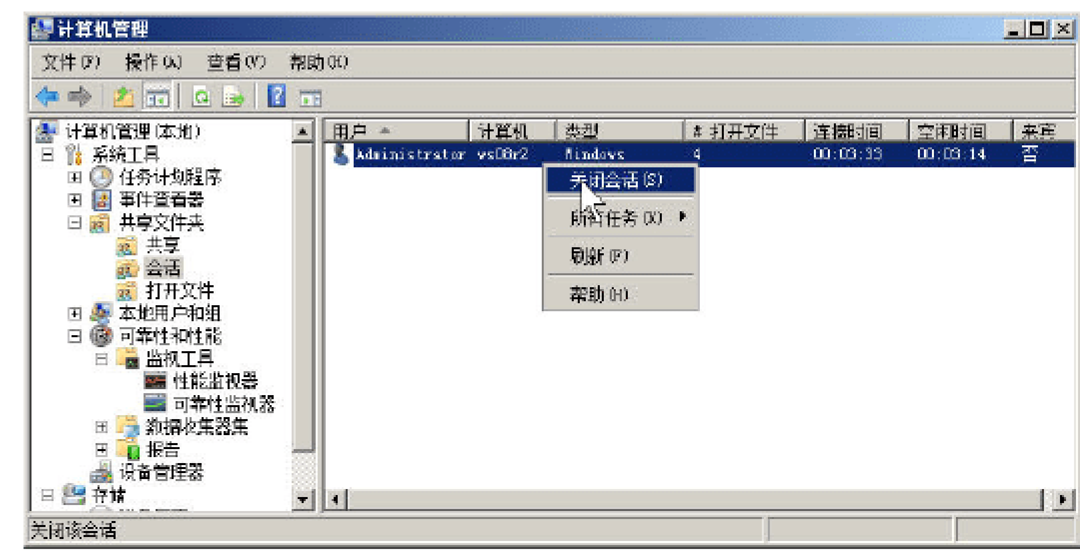


图 2-73　会话

03 在“共享文件夹→打开文件”中，显示了连接到该计算机提供的共享，并通过共享文件夹使用中的文件，也可以选中打开的文件，在右键菜单中，关闭这些打开的文件，如图 2-74 所示。

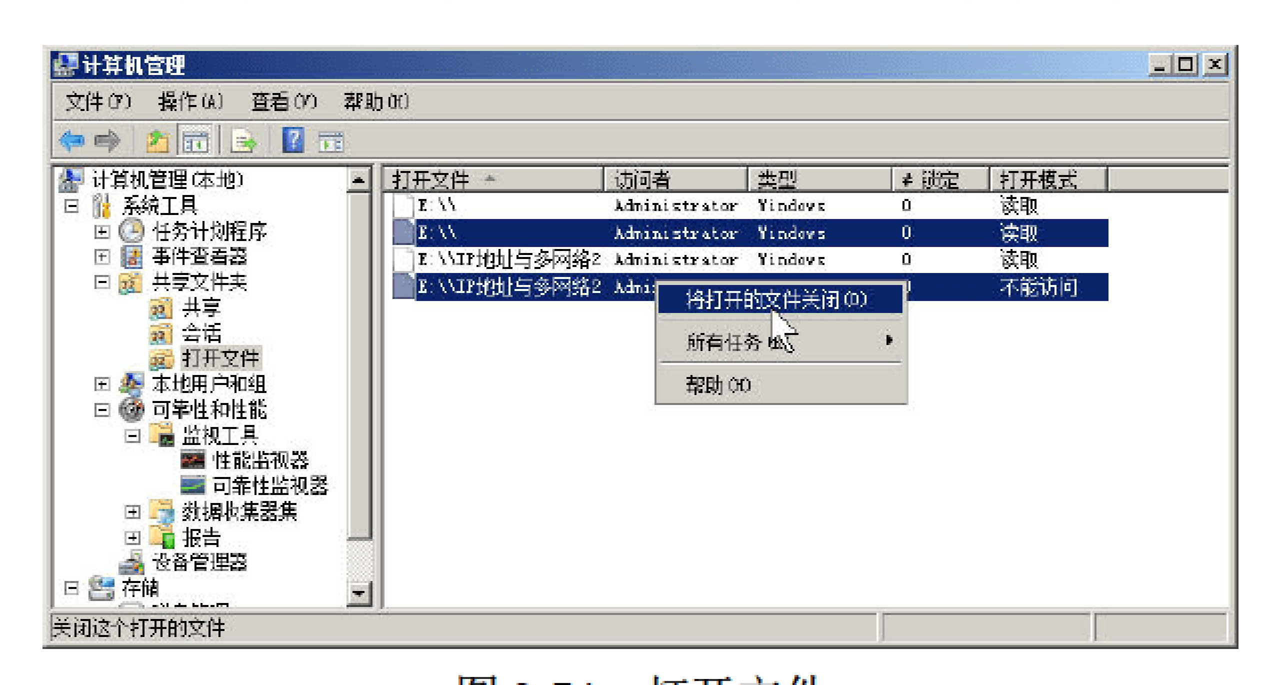


图 2-74　打开文件

2.6.5　其他组件

“计算机管理”还包括“可靠性和性能”、“设备管理器”、“磁盘管理”、“服务”、“路由和远程访问服务”等组件，下面简要介绍。

（1）可以使用“可靠性和性能”监视器实时检查影响计算机性能运行程序的因素，并通过收集日志数据供以后分析使用。“可靠性和性能”包括“监视工具”、“数据收集器集”、“报告”三组程序。其中“监视工具”包括“性能监视器”和“可靠性监视器”。Windows 可靠性和性能

监视器使用时合并进了数据收集器集的性能计数器、事件跟踪数据和配置信息。可靠性和性能管理界面如图 2-75 所示。

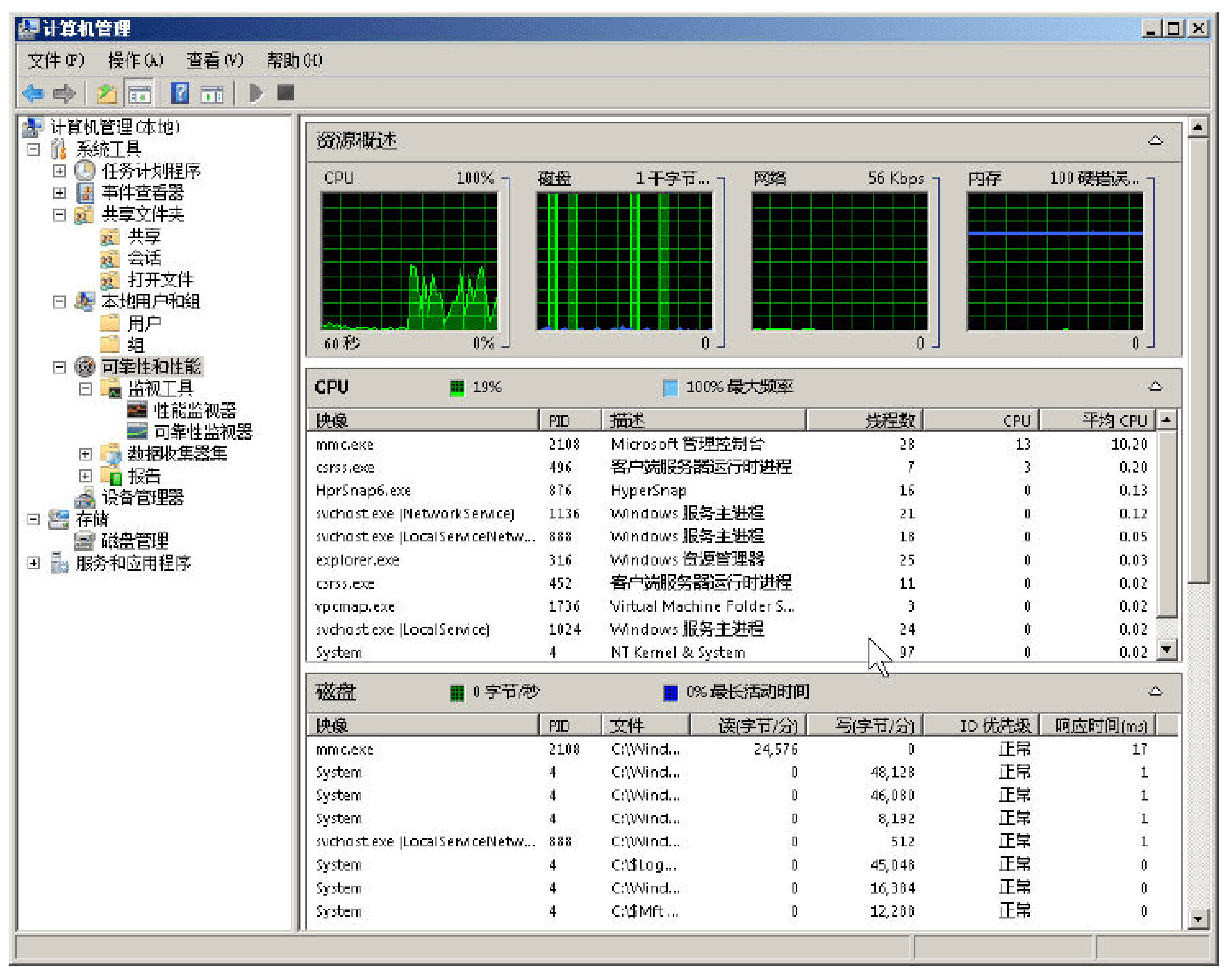


图 2-75　可靠性和性能

（2）“设备管理器”组件的内容请参考“2.5.2　设备管理器”。

（3）“磁盘管理”中，可使用此版本的 Windows 中的磁盘管理来执行与磁盘相关的任务，如创建、格式化分区和卷，以及分配驱动器号。另外，可以使用 DiskPart 命令和其他命令行实用工具来执行磁盘管理任务。有关“磁盘管理”的内容，将在后面的章节单独介绍。

（4）Windows Server 2008 中的“路由和远程访问”服务使用虚拟专用网络（VPN）或拨号连接支持远程用户连接或站点间连接。“路由和远程访问”包含下列组件。

- 远程访问：远程访问功能提供 VPN 服务，使用户可以通过 Internet 访问公司网络，如同他们直接连接到公司网络上。远程访问还允许使用拨号通信链路的远程工作人员或流动工作人员访问公司网络。
- 路由：“路由和远程访问”是用于路由和联网的一个全功能软件路由器和开放平台，为局域网（LAN）和广域网（WAN）环境中的公司提供路由服务，或使用安全的 VPN 连接通过 Internet 提供路由服务。路由用于多协议 LAN-to-LAN、LAN-to-WAN、VPN 和网络地址转换（NAT）服务。

（5）可以使用“服务”管理单元管理在本地或远程计算机上运行的服务，如停止或启动服务，如图 2-76 所示。也可以使用 sc config 命令管理服务。

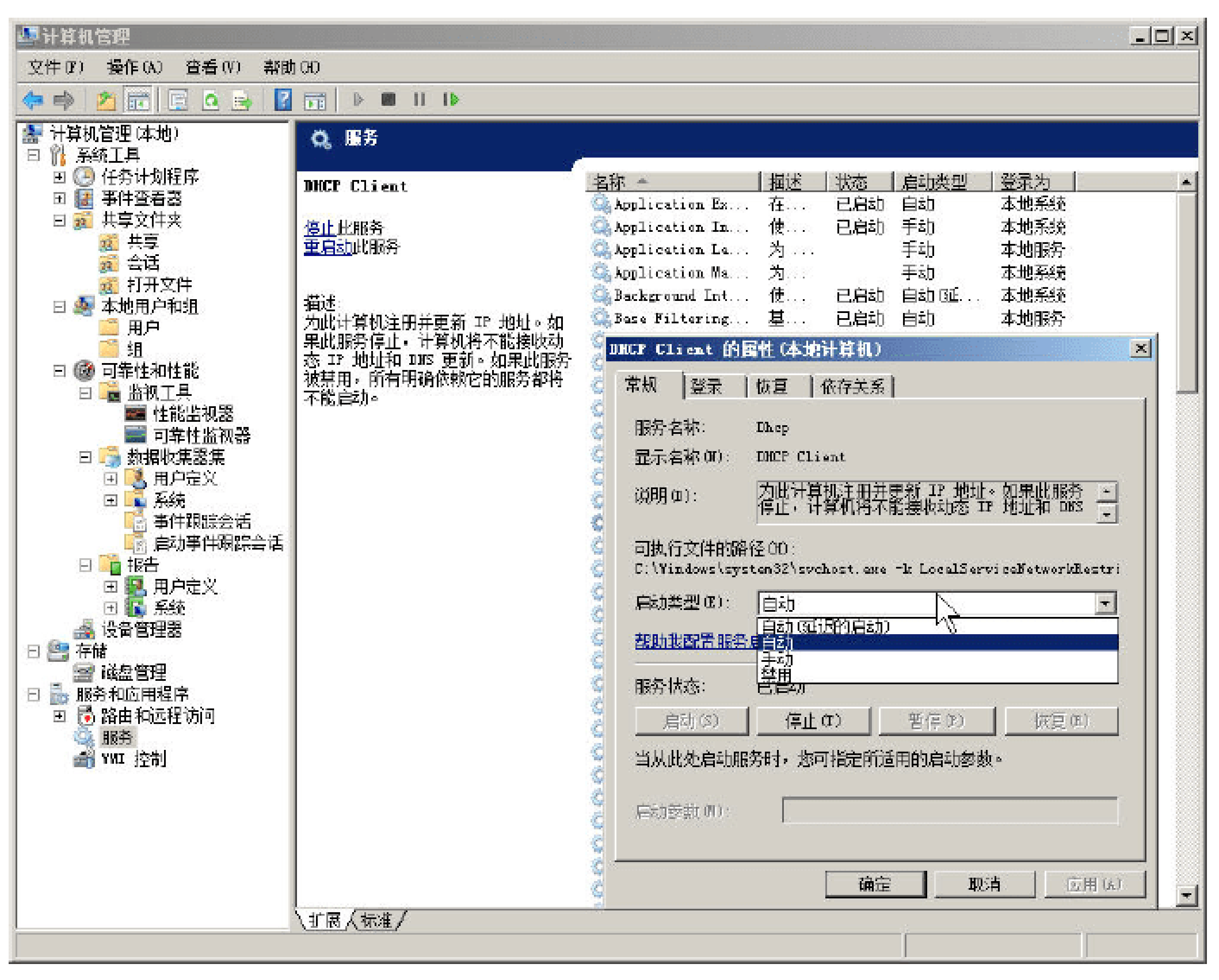


图 2-76　服务

2.7　本地用户和组

“本地用户和组”管理控制台用于创建并管理存储在本地计算机上的用户和组。“本地用户”和“本地用户组”位于“计算机管理”中，用户可以使用这一组管理工具来管理单台本地或远程计算机。可以使用本地用户和组保护并管理存储在本地计算机上的用户账户和组。可以在特定计算机上（只能是这台计算机）分配本地用户账户或组账户的权限和权利。

通过本地用户和组，可以为用户和组分配权利和权限，从而限制用户和组执行某些操作的能力。权限可授权用户在计算机上执行某些操作，如备份文件和文件夹或者关机。权限是与对象（通常是文件、文件夹或打印机）相关联的一种规则，它规定哪些用户可以访问该对象以及以何种方式访问。简单来说，用户与用户组的功能与用途如下。

（1）单独的“用户”或“组”没有意义。只有将“用户”或“组”与“资源”进行“绑定”时才有意义。这里面的“资源”，可以是作为服务器端所属计算机上的设备，如以共享文件夹方式提供的磁盘空间，或者打印机“共享打印机”。

（2）在分配资源或者配置资源的属性时，可以根据不同的“用户”或“组”设置不同的权限，如“读”、“写”、“完全控制”等权限。

（3）在使用“本地用户”或“本地组”的计算机时，它们之间采用的是“对等网”的网络方式。所谓“对等网”，是指网络中的计算机，没有提供统一身份验证的服务器，用户想要访问哪个设备，就需要有对方提供的用户名及对应的密码。例如，网络中有 A、B、C 三台计算机，如果 C 要访问（或使用）A、B 提供的资源，则 C 就需要有 A、B 所提供的用户名及对应的密码。当然，对于 A 或 B 来说，为 C 提供的用户名或密码，可以相同，也可以不同。在“对等网”之间，网络关系是“单向”的。例如，在上例中，A、B 为 C 提供资源，如果 A 想要访问 B，B 也必须为 A

提供对应的访问用户名及密码。

对等网能提供的访问资源、性能是有限的，在“对等网”中，每个提供服务的“服务端”，最多允许 10 个客户同时访问。从本质上来说，对等网，是一个比较简单的、适合小范围局域网使用的网络，它们的关系也是简单的“二层”关系：网络资源与“用户”或“组”相对应，并对“用户”与“组”设置不同的权限。



说 明

所有的 Windows 95 及其以后的 Windows 操作系统，无论是服务器操作系统还是工作站操作系统，都可以做“对等网”的服务器端或客户端，并不仅限于 Windows Server 2003、Windows Server 2008 等服务器操作系统。

2.7.1　默认本地用户账户概述

“本地用户和组”管理单元中的“用户”文件夹显示默认的用户账户以及创建的用户账户。这些默认的用户账户是在安装操作系统时自动创建的。表 2-2 描述了显示在本地用户和组中的每个默认用户账户。

表 2-2　系统默认用户账户

默认用户账户	描述
Administrator 账户	对于 Windows 7、Windows Vista 等操作系统来说，在默认情况下，Administrator 账户处于禁用状态，但也可以启用它。当它处于启用状态时，Administrator 账户具有对计算机的完全控制权限，并可以根据需要向用户分配用户权利和访问控制权限。该账户必须仅用于需要管理凭据的任务。强烈建议将此账户设置为使用强密码 Administrator 账户是计算机上 Administrators 组的成员。不可以从 Administrators 组删除 Administrator 账户，但可以重命名或禁用该账户。由于大家都知道 Administrator 账户存在于许多版本的 Windows 上，所以重命名或禁用此账户将使恶意用户尝试并访问该账户变得更为困难 即使已禁用了 Administrator 账户，仍然可以在安全模式下使用该账户访问计算机
Guest 账户	Guest 账户由在这台计算机上没有实际账户的人使用。如果某个用户的账户已被禁用，但还未删除，那该用户也可以使用 Guest 账户。Guest 账户不需要密码。默认情况下，Guest 账户是禁用的，但也可以启用它 可以像任何用户账户一样设置 Guest 账户的权利和权限。默认情况下，Guest 账户是默认的 Guest 组的成员，该组允许用户登录计算机。其他权利及任何权限都必须由 Administrators 组的成员授予 Guests 组。默认情况下将禁用 Guest 账户，并且建议将其保持禁用状态

2.7.2　默认本地组概述

“本地用户和组”管理控制台中的“组”文件夹默认显示本地组以及创建的本地组。默认本地组是在安装操作系统时自动创建的。如果一个用户属于某个本地组，则该用户就具有在本地计算机上执行各种任务的权利和能力。可以向本地组添加本地用户账户、域用户账户、计算机账户以及组账户。

表 2-3 提供了对位于组文件夹中的默认组的描述。此表也列出了每个组的默认用户权利，这些用户权利是在本地安全策略中分配的。

表 2-3　系统默认本地组

组	描述	默认用户权利
Administrators	此组的成员具有对计算机的完全控制权限，并且他们可以根据需要向用户分配用户权利和访问控制权限。Administrator 账户是此组的默认成员。当计算机加入域中时，Domain Admins 组会自动添加到此组中。因为此组可以完全控制计算机，所以向其中添加用户时要特别谨慎	从网络访问此计算机 调整进程的内存配额 允许本地登录 允许通过终端服务登录 备份文件和目录 跳过遍历检查 更改系统时间 更改时区 创建页面文件 创建全局对象 创建符号链接 调试程序 从远程系统强制关机 身份验证后模拟客户端 提高日程安排的优先级 装载和卸载设备驱动程序 作为批处理作业登录 管理审核和安全日志 修改固件环境变量 执行卷维护任务 配置单一进程 配置系统性能 从扩展坞中取出计算机 还原文件和目录 关闭系统 获得文件或其他对象的所有权
Backup Operators	此组的成员可以备份和还原计算机上的文件，而不管保护这些文件的权限如何。这是因为执行备份任务的权利要高于所有文件权限。此组的成员无法更改安全设置	从网络访问此计算机 允许本地登录 备份文件和目录 跳过遍历检查 作为批处理作业登录 还原文件和目录 关闭系统
Cryptographic Operators	已授权此组的成员执行加密操作	没有默认的用户权利
Distributed COM Users	允许此组的成员在计算机上启动、激活和使用 DCOM 对象	没有默认的用户权利
Guests	该组的成员拥有一个在登录时创建的临时配置文件，在注销时，此配置文件将被删除。来宾账户（默认情况下已禁用）也是该组的默认成员	没有默认的用户权利
IIS_IUSRS	这是 Internet 信息服务（IIS）使用的内置组	没有默认的用户权利
Network Configuration Operators	该组的成员可以更改 TCP/IP 设置，并且可以更新和发布 TCP/IP 地址。该组中没有默认的成员	没有默认的用户权利
Performance Log Users	该组的成员可以从本地计算机和远程客户端管理性能计数器、日志和警报，而不用成为 Administrators 组的成员	没有默认的用户权利
Performance Monitor Users	该组的成员可以从本地计算机和远程客户端监视性能计数器，而不用成为 Administrators 组或 Performance Log Users 组的成员	没有默认的用户权利

（续表）

组	描述	默认用户权利
Power Users	默认情况下，该组的成员拥有不高于标准用户账户的用户权利或权限。在早期版本的 Windows 中，Power Users 组专门为用户提供特定的管理员权利和权限，执行常见的系统任务。在此版本 Windows 中，标准用户账户具有执行最常见配置任务的能力，例如更改时区。对于需要与早期版本的 Windows 相同的 Power User 权利和权限的旧应用程序，管理员可以应用一个安全模板，此模板可以启用 Power Users 组，以假设具有与早期版本的 Windows 相同的权利和权限	没有默认的用户权利
Remote Desktop Users	该组的成员可以远程登录计算机	允许通过终端服务登录
Replicator	该组支持复制功能。Replicator 组的惟一成员应该是域用户账户，用于登录域控制器的复制器服务。不能将实际用户的用户账户添加到该组中	没有默认的用户权利
Users	该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定计算机。该组的成员无法共享目录或创建本地打印机。默认情况下，Domain Users、Authenticated Users 以及 Interactive 组是该组的成员。因此，在域中创建的任何用户账户都将成为该组的成员	从网络访问此计算机 允许本地登录 跳过遍历检查 更改时区 增加进程工作集 从扩展坞中取出计算机 关闭系统
提供远程协助帮助程序	该组的成员可以向此计算机用户提供远程协助	没有默认的用户权利

2.7.3　本地用户管理

在本小节中，我们介绍在 Windows Server 2008 中，管理“本地用户”的方法与步骤，包括创建“用户”、删除“用户”、为“用户”修改密码、将用户加入到“组”等内容。

01 在“计算机管理”中，定位到“系统工具→本地用户和组→用户”，在右侧的空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新用户”选项，如图 2-77 所示，进入创建用户向导页面。

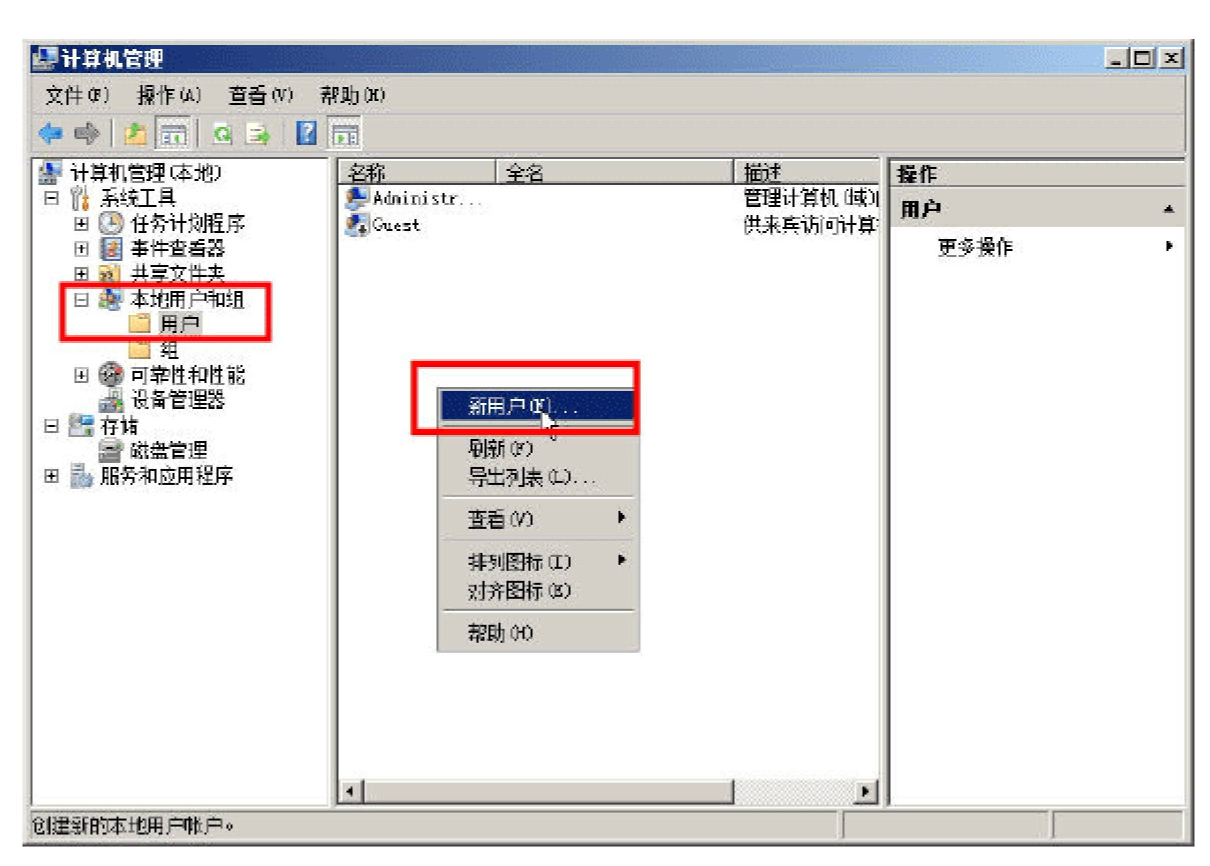


图 2-77　新用户

02 在弹出的“新用户”对话框中，输入用户名、全名、描述、密码等信息，并且根据需要，选择创建用户的选项。其中“用户名”是必须输入的，其他可以为空或保持默认值。在选择“用户名”时，推荐以英文的字母开头，并且可以根据需要，使用下划线、短横线、数字等信息。在本例中，设置用户名为 ws01，密码设置为 1234，如图 2-78 所示。

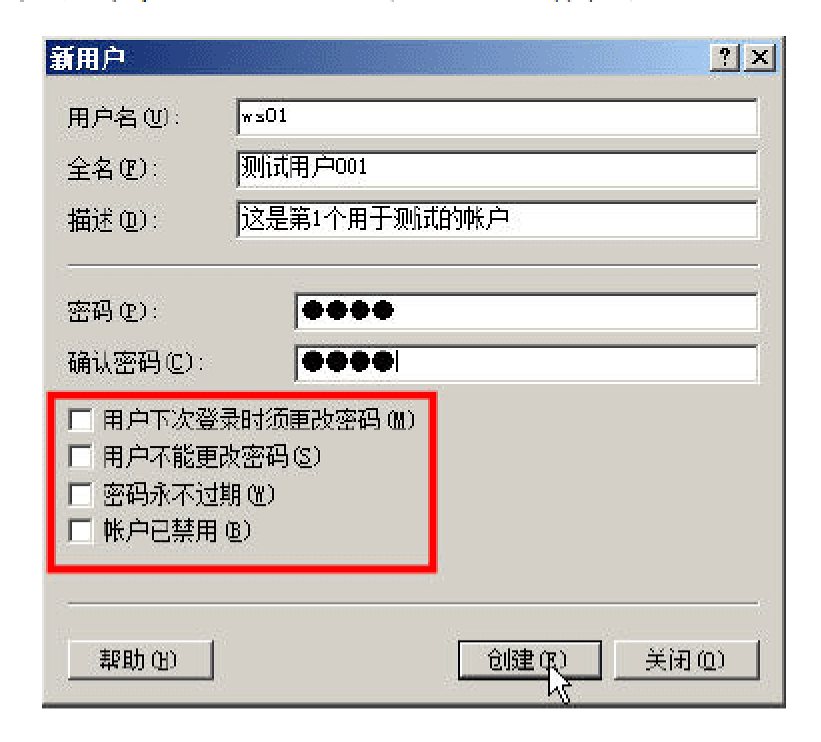


图 2-78 创建用户

创建用户各选项意义如下。

- 如果选中“用户下次登录时须更改密码”，则使用该用户登录到计算机（或登录到网络），或者通过网络访问该服务器时，则需要修改密码。
- 如果选中“用户不能更改密码”，则用户不能修改密码。
- 如果选中“密码永不过期”，则该用户密码将不会过期。如果不选中本项，在默认情况下，用户的密码将会在 42 天后过期。
- 如果选中“账户已禁用”，则该账户将不能使用。

请根据需要，输入创建的用户信息，选择用户的选项，确定之后，单击“创建”按钮。

03 创建用户之后，可以输入新的用户名、用户全名、描述信息、密码，继续创建用户，或者单击“关闭”按钮，关闭“新用户”对话框，如图 2-79 所示。

04 关闭“新用户”对话框后，返回到“计算机管理→系统工具→本地用户和组→用户”，在右侧列表中，可以看到当前系统中已经存在的用户。如果要修改用户的选项，或者对用户进行操作，可以用鼠标右击选中用户，在弹出的对话框中，根据需要选择“删除—删除选择的用户”、“重命名—修改用户名”、“设置密码—修改用户密码”或“属性-打开用户属性对话框，修改用户属性”，如图 2-80 所示。

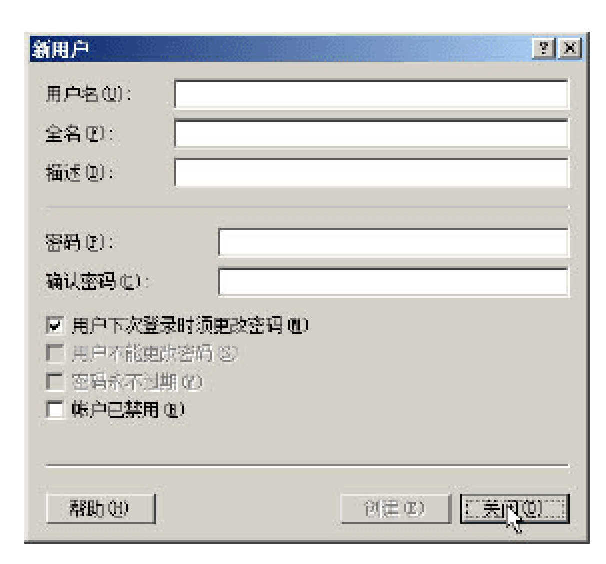


图 2-79 新用户

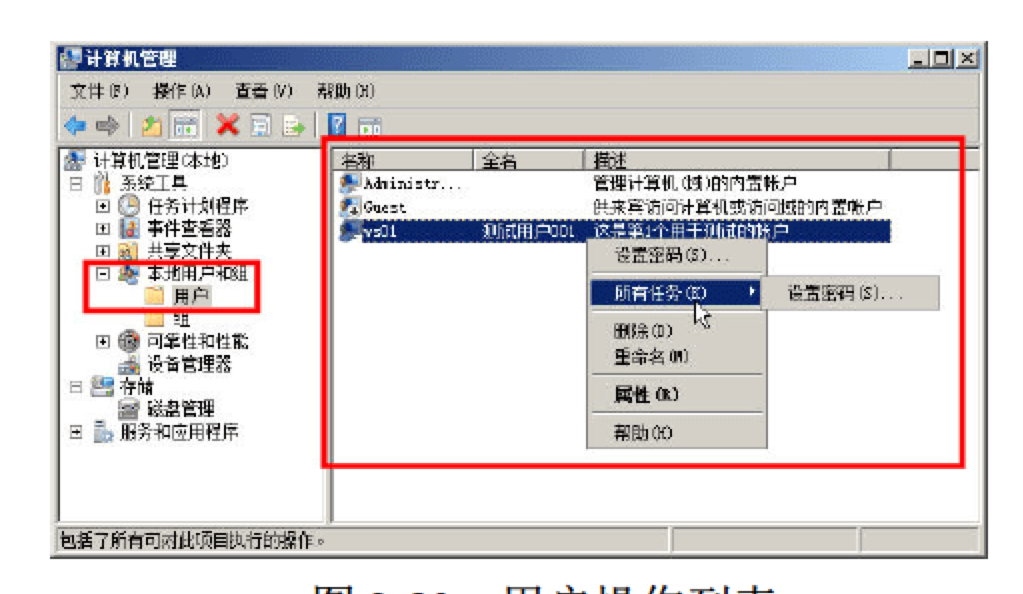


图 2-80 用户操作列表

05 如果要为用户修改密码，会弹出如图 2-81 所示的对话框，单击“继续”按钮，在弹出的新对话框中，为用户修改密码即可，如图 2-82 所示。

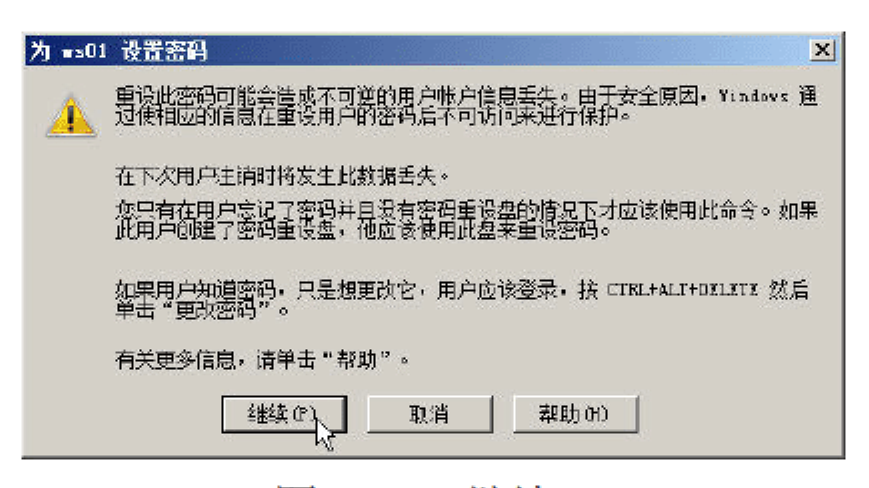


图 2-81　继续

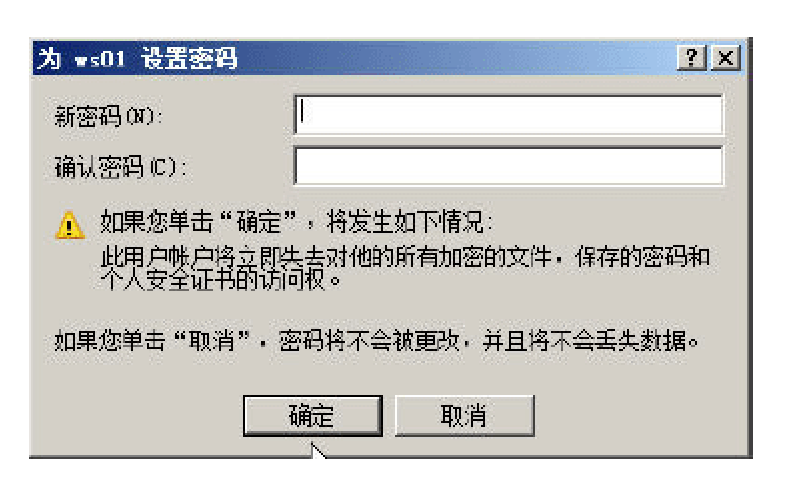


图 2-82　设置新密码

06 如果打开用户属性，在“隶属于”选项卡中，可以将用户添加到其他用户组中，单击“添加”按钮，在弹出的对话框中，单击“高级”按钮，如图 2-83 所示。

07 此时“选择组”对话框将更改为图 2-84 所示的页面，单击“立即查找”按钮，系统将浏览当前计算机中所有的用户组，并在“搜索结果”中显示，可以选择要将当前用户加入到的组（按住 Shift 或 Ctrl 键并用鼠标单击选择一个或多个组），选择之后单击“确定”按钮。

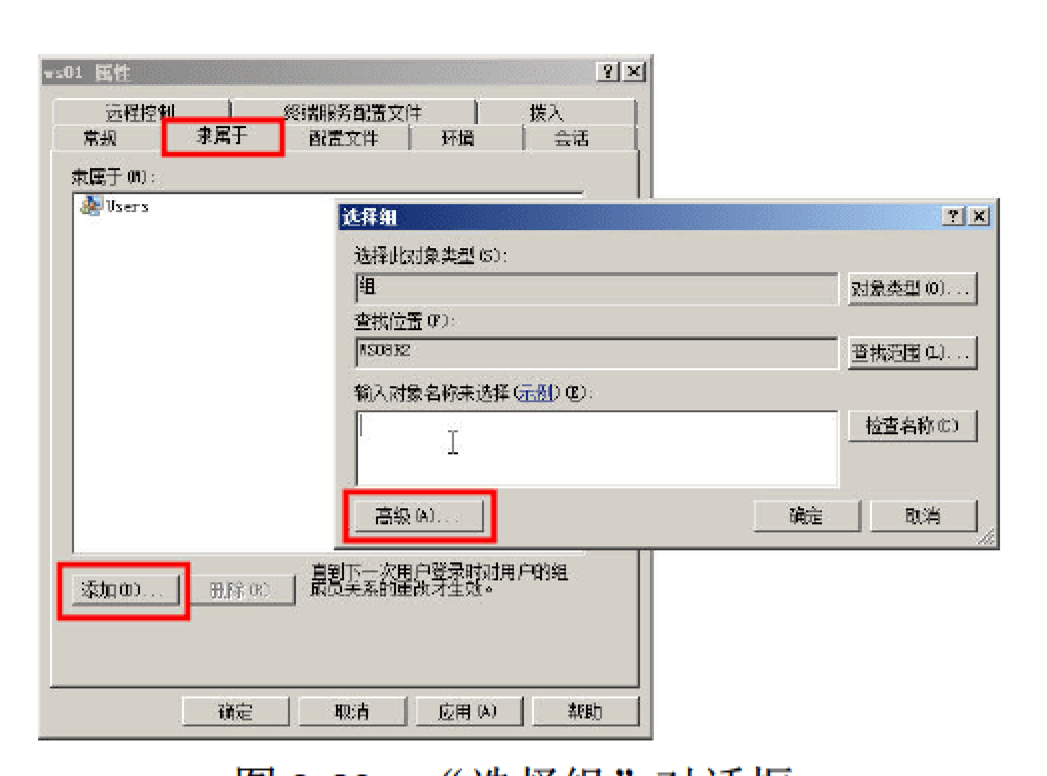


图 2-83　“选择组”对话框

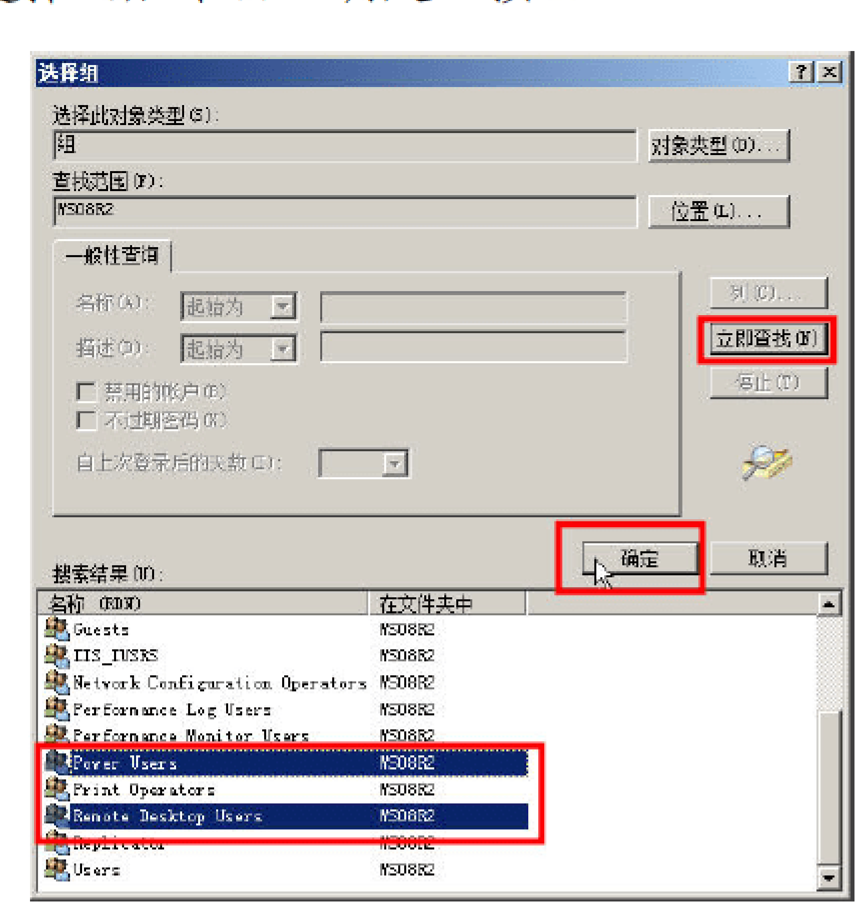


图 2-84　选择要加入到的用户组

08 随后会返回到“选择组”对话框，在“输入对象名称来选择”列表中，显示了图 2-84 中选中并添加的用户，如图 2-85 所示。单击“确定”按钮，完成选择。

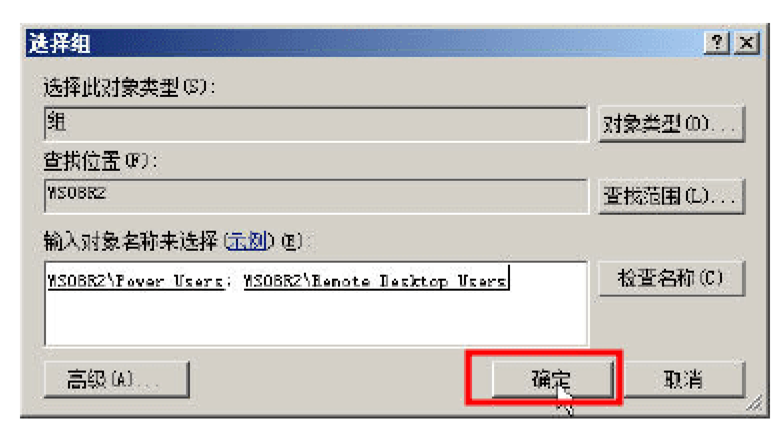


图 2-85　选择用户完成



说　明

如果知道要加入到的“组”，可以直接在“输入对象名称来选择”列表中，输入要添加到的组，如果有多个组，可以用英文的“分号”分隔。

09 返回到“隶属于”选项卡，可以看到添加的列表，单击“确定”按钮返回，完成添加操作，如图 2-86 所示。

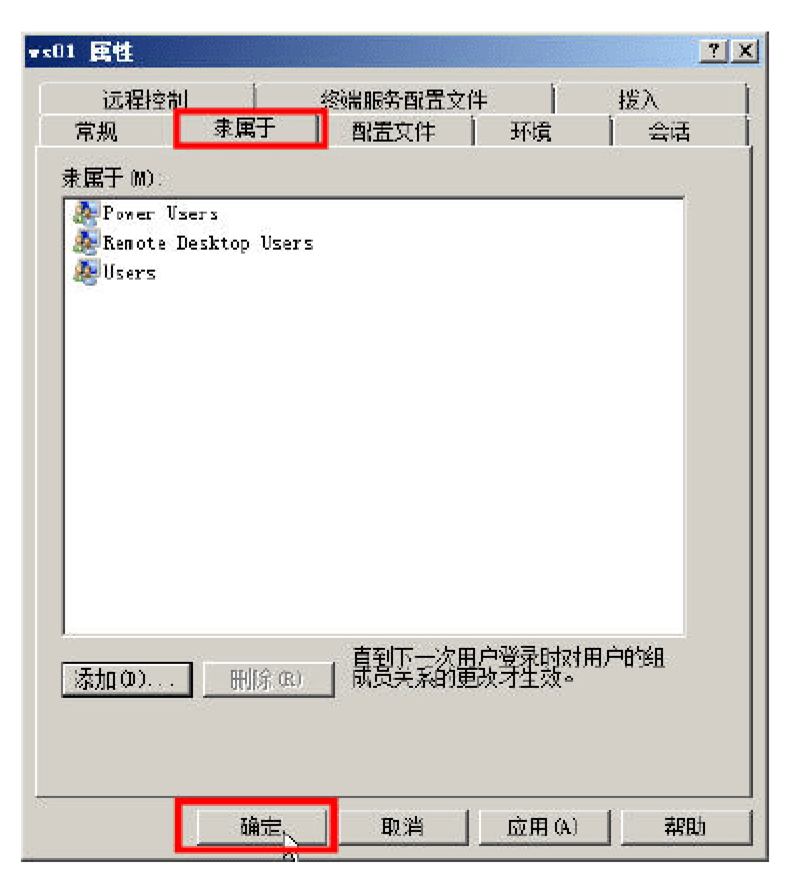


图 2-86　添加组



说 明

如果要从用户中删除用户组，可以在图 2-86 所示的对话框中，选中要删除的用户组，然后单击“删除”按钮即可。

2.7.4　组管理

本小节介绍“组”管理的内容，操作步骤如下。

01 在“计算机管理”中，定位到“系统工具→本地用户和组→组”，在右侧的空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建组”，如图 2-87 所示，进入创建用户向导页。

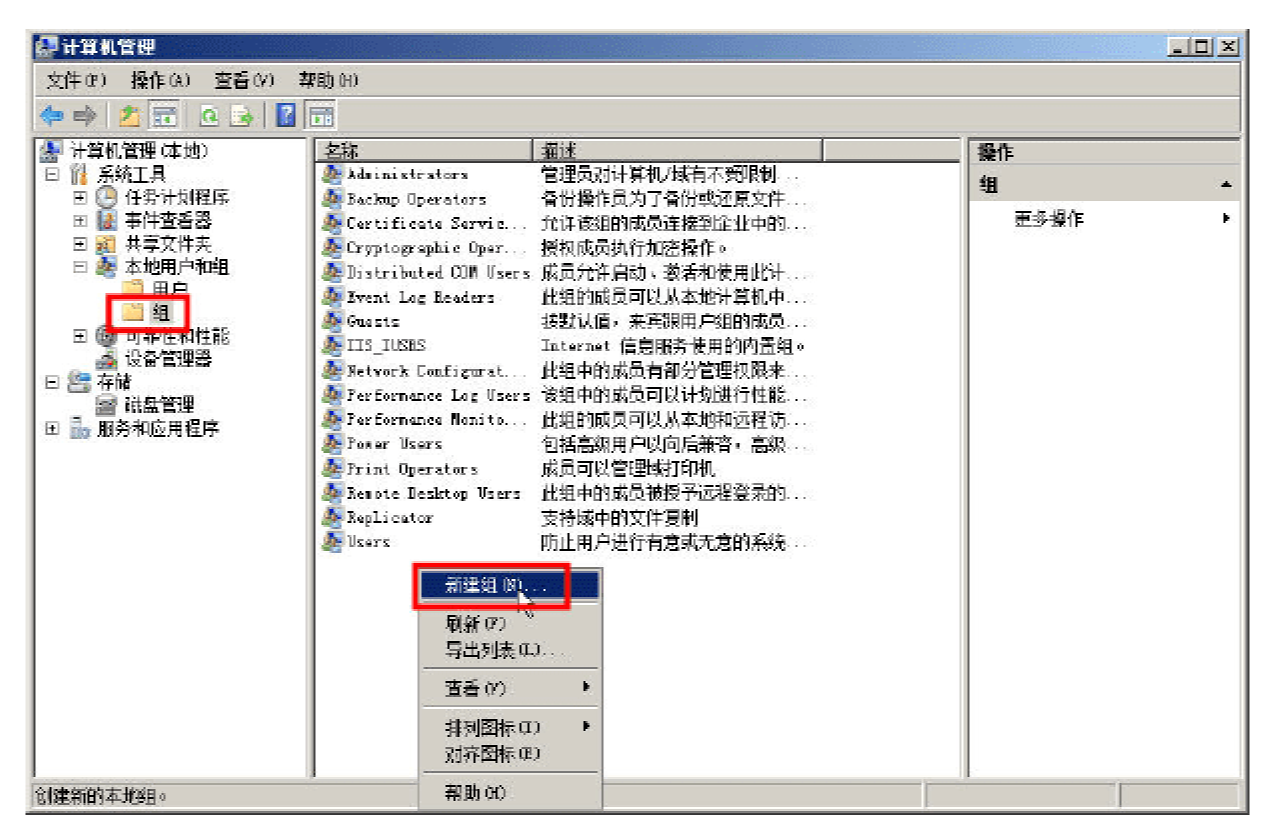


图 2-87　新建组

02 在弹出的“新建组”对话框中，输入“组名”（必须输入），以及“描述信息”（根据需要输入），在创建组的时候，如果要向组中添加用户，可以单击“添加”按钮，选择要添加的用户。设置之后单击“创建”按钮，如图 2-88 所示。



图 2-88　创建用户

03 与“用户”的操作类似，“组”也有重命名、删除、修改属性等操作，但不能为“组”设置密码。可以在“组”中添加多个“用户”，也可以将“用户”添加到多个不同的“组”，用户与组是“多对多”的关系。在“组”中也可以添加其他“组”。向“组”中添加用户的操作如图 2-89 所示，这与向“用户”中添加“组”的操作类似。

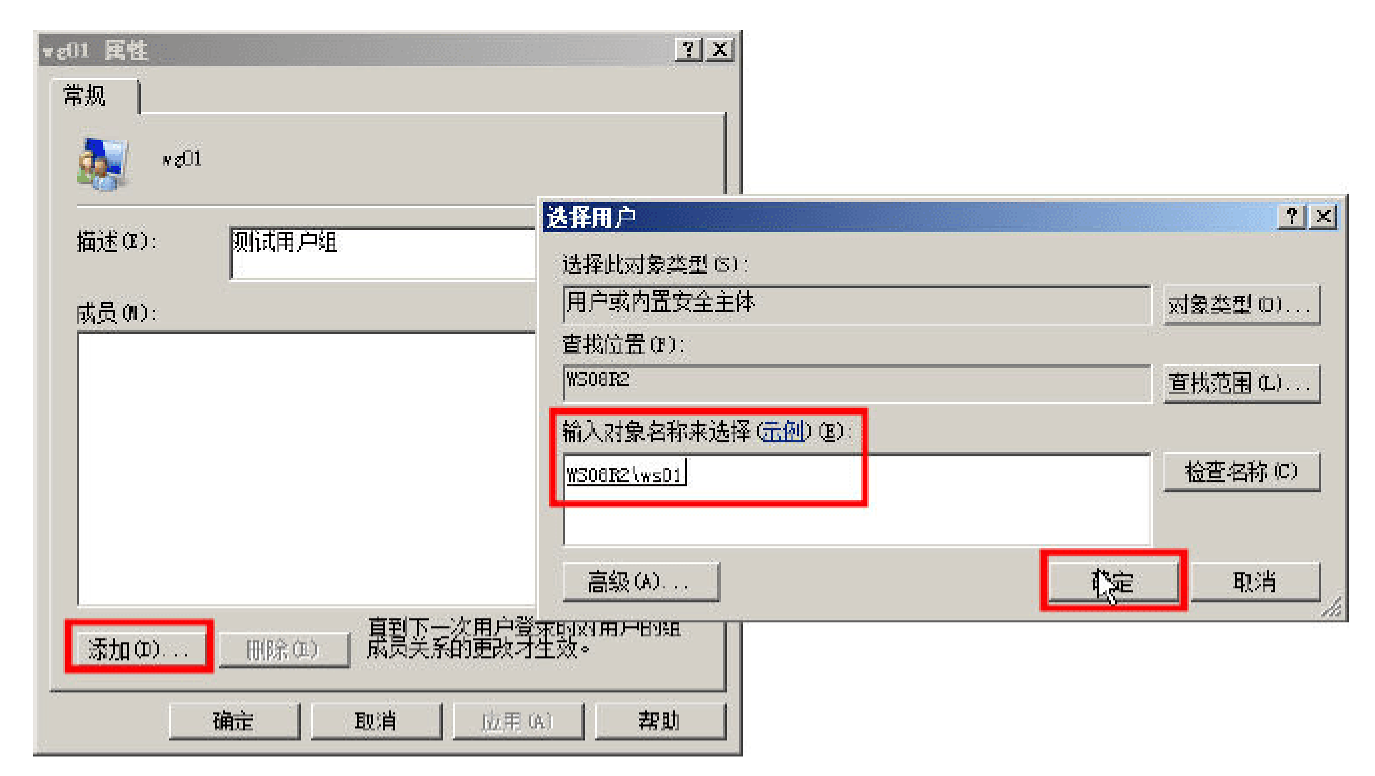


图 2-89　向组中添加用户

第 3 章　基本网络服务管理

DHCP、DNS 是网络中最基本的服务，前者可以为网络中的计算机或其他网络设备分配 IP 地址等参数，后者可以提供域名到 IP 地址的解析工作。而 WINS 则是 Windows 网络所特有的网络服务，可以提供从 NetBIOS 名称到 IP 地址的解析工作。

DHCP、DNS 和 WINS 服务器，都是典型的“客户/服务器”系统（或简称 C/S 系统），包括服务器端和客户端。一般情况下，提供服务的一端，是服务器端，而需要 IP 地址、名称解析的一端则是客户端。

本章将介绍基于 Windows Server 2008 R2 中 DHCP、DNS 和 WINS 服务器的内容，包括服务器的概述、安装配置、在网络中的使用以及使用注意事项等。

3.1　DHCP 概述

如今是网络时代，单位中的计算机大多需要连接到网络，这就需要为计算机设置 IP 地址、子网掩码、网关地址和 DNS 地址，有时还需要设置 WINS 服务器地址。当网络中有几十台甚至更多台计算机时，如果网管为每台计算机手动设置这些 TCP/IP 地址及其参数，对网管来说将是极大的负担。这时候就需要 DHCP 服务为网管分担这些任务。

DHCP（Dynamic Host Configure Protocol，动态主机配置协议）服务在网络中起着重要的作用，它可以为网络中的计算机自动分配 TCP/IP 地址、子网掩码、网关地址、DNS 地址和 WINS 服务器地址等参数，使用 DHCP 服务器，可以极大地减轻网管的负担。

DHCP 是一种 IP 标准，其设计目的是通过集中管理网络上使用的 IP 地址和相关配置细节来降低管理计算机网络中地址配置的复杂性。Microsoft 公司从 Windows NT Server 开始提供 DHCP 服务器，可以为网络上的计算机自动分配 IP 地址及相关参数。

3.1.1　使用 DHCP 服务的好处

TCP/IP 网络上的每台计算机都必需有惟一的 IP 地址。IP 地址（以及和之相关的子网掩码）可以标识主机及其连接的子网。如果将计算机移动到不同的子网，则必需更改 IP 地址。DHCP 允许用户通过本地网络上的 DHCP 服务器的 IP 地址数据库为客户端动态指派 IP 地址。使用 DHCP 管理基于 TCP/IP 的网络具有以下几大优势：

- 安全而可靠的配置。DHCP 避免了由于在每台计算机上进行手动配置而引起的错误。此外，DHCP 还可以防止由于在网络上配置新的计算机时重用已指派的 IP 地址而引起的地址冲突。
- 减少配置管理。如果手动设定网络中每台计算机的 IP 地址、子网掩码、网关地址、DNS 地址、WINS 服务器地址等参数，将占用管理员大量的时间。而使用 DHCP 服务器可以大大降低用于配置和重新配置网上计算机的时间。
- 为需要经常更改网络参数的用户提供方便。使用笔记本办公或频繁更改位置的用户，在每次更换位置后，都需要重新配置上网参数。而 DHCP 租约续订过程解决了这个问题。
- 在采用 Windows 部署服务（远程安装服务）或使用其他 TFTP 服务器时，DHCP 服务器是必需的。

3.1.2　DHCP 的工作原理

本节通过一台计算机自动获取 IP 地址的过程，简述 DHCP 的工作原理。

1．寻找 DHCP 服务器

当 DHCP 客户端第一次启动网络组件时，如果客户端发现本机上没有任何 IP 地址等相关参数，它会向网络上发出一个 DHCPDISCOVER 数据包。这个数据包的源地址为 0.0.0.0，而目的地址则为 255.255.255.255，然后再加上 DHCPDISCOVER 的信息，向整个网络进行广播。

在 Windows 的预设情况下，DHCPDISCOVER 的等待时间预设为 1 秒，也就是当客户端将第一个 DHCPDISCOVER 包送出去之后，在 1 秒内如果没有得到回应的话，就会进行第二次 DHCPDISCOVER 广播。如果一直得不到回应，客户端将在 16 秒内广播 4 次 DHCPDISCOVER。如果都没有得到 DHCP 服务器的响应，客户端会显示错误信息，宣告 DHCPDISCOVER 发送失败。此时，DHCP 客户端会从 169.254.0.1～169.254.255.254 自动获取一个地址，并设置子网掩码为 255.255.0.0，系统会在 5 分钟之后再重复一次 DHCPDISCOVER 的过程。

2．提供 IP 租用地址

当 DHCP 服务器收到客户端发出的 DHCPDISCOVER 广播后，它会从可用地址中选择最前面的 IP，连同其他 TCP/IP 设定（包括子网掩码、网关地址、DNS 地址、WINS 服务器地址等参数），回应给客户端一个 DHCPOFFER 包。

由于客户端在开始时还没有 IP 地址，所以在其 DHCPDISCOVER 包内会带有其 MAC 地址信息，并且有一个 XID 编号来辨别该包。DHCP 服务器返回的 DHCPOFFER 数据包则会根据这些资料传递给要求租用的客户。根据服务器端的设定，DHCPOFFER 包会包含一个租约期限的信息。

3．接受 IP 租约

如果客户端收到网路上多台 DHCP 服务器的回应，则会从中选择一个 DHCPOFFER（通常是最先到达的那个），并且会向网络上发送一个 DHCPREQUEST 广播数据包，告诉所有 DHCP 服务器它将指定接受哪一台服务器提供的 IP 地址。

同时，客户端还会向网络发送一个 ARP（Address Resolution Protocol，地址解析协议）包，查

询网络上面有没有其他机器使用该 IP 地址；如果发现该 IP 已经被占用，客户端则会送出一个 DHCPDECLINE 数据包给 DHCP 服务器，拒绝接受其 DHCPOFFER，并重新发送 DHCPDISCOVER 信息。

4．租约确认

当 DHCP 服务器接收到客户端的 DHCPREQUEST 之后，会向客户端发出一个 DHCPACK 回应，以确认 IP 租约的正式生效，也就结束了一个完整的 DHCP 工作过程。

DHCP 服务器分配的 IP 地址是有租约限制的，默认情况下是 8 天。DHCP 客户端在其租约剩余一半的时候会发出 DHCPREQUEST，如果此时得不到 DHCP 服务器确认的话，工作站还可以使用这个 IP 地址。当在租约到达 75%时，如果还得不到确认的话，则工作站就会放弃使用此地址，开始新一轮的申请。

DHCP 服务器是以广播方式进行的，这就需要在每一个子网中安装一台 DHCP 服务器。如果想使用一台 DHCP 服务器为所有子网的工作站分配 IP 地址，则需要在每个子网中配置（或安装）DHCP 中继服务器。现在的三层交换机都支持 DHCP 中继。

3.1.3　DHCP 服务的相关概念

在学习使用 DHCP 服务器的过程中，先介绍以下名词的含义。

1．作用域

作用域是网络上可用 IP 地址的完整连续范围。作用域通常定义为接受 DHCP 服务的网络上的单个物理子网。作用域还为网络上的客户端提供服务器对 IP 地址及任何相关配置参数的分发和指派进行管理的主要方法。

2．超级作用域

超级作用域是作用域的管理组合，它可用于支持同一物理子网上的多个逻辑 IP 子网。超级作用域仅包含可同时激活的“成员作用域”或“子作用域”列表。超级作用域不用于配置有关作用域使用的其他详细信息。如果想配置超级作用域内使用的多种属性，用户需要单独配置成员作用域属性。

3．排除范围

排除范围是作用域内从 DHCP 服务中排除的有限 IP 地址序列。排除范围确保服务器不会将这些范围中的任何地址提供给网络上的 DHCP 客户端。例如，如果设置的地址范围是 172.16.1.1～172.16.1.254，同时设置了排除范围为 172.16.1.50～172.16.1.100，那么该 DHCP 服务器不会将 172.16.1.50～172.16.1.100 范围内的 IP 地址出租给客户端。

4．地址池

在定义了 DHCP 作用域并应用排除范围之后，在作用域内剩余的地址便是“地址池”。DHCP 服务器可将池内地址动态地指派给网络上的 DHCP 客户端。例如，当在 172.16.1.1～172.16.1.254 范围内设置了排除范围 172.16.1.50～172.16.1.100 后，地址池将变成 172.16.1.1～172.16.1.49 和

172.16.1.101～172.16.1.254。

5. 租约

租约是由 DHCP 服务器指定的一段时间，在此时间内客户端计算机可使用指派的 IP 地址。当向客户端提供租约时，租约是“活动”的。在租约过期之前，客户端通常需要向服务器更新指派给它的地址租约。当租约期满或在服务器上被删除时，它将变成“非活动”的。租约期限决定租约何时期满以及客户端需要向服务器对它进行更新的频率。

6. 保留

可使用“保留”功能来创建 DHCP 服务器指派的永久地址租约。“保留”可确保子网上指定的硬件设备始终可使用相同的 IP 地址。

7. 选项类型

“选项类型”是 DHCP 服务器在向 DHCP 客户端提供租约时可指派的其他客户端配置参数。例如，一些常用选项包含用于默认网关（路由器）、WINS 服务器和 DNS 服务器的 IP 地址。通常，为每个作用域启用并配置这些选项类型。DHCP 控制台还允许用户配置由服务器添加和配置的所有作用域使用的默认选项类型。例如，用于 PXE 的无盘工作站或者使用“Windows 部署服务”，需要将 DHCP 选项 60 配置为“PXEClient”。

8. 选项类别

“选项类别”是一种可供服务器进一步管理提供给客户端的选项类别的方式。当选项类别添加到服务器时，可为该类别的客户端提供用于其配置类别的特定选项类型。对于 Windows 2000 和 Windows XP，客户端计算机还可以在和服务器通信时指定类 ID。对于不支持类 ID 过程的早期 DHCP 客户端，当需要将客户端归类时可以把服务器配置成默认类以便使用。选项类有两种类别：供应商类别和用户类别。

3.1.4　大型网络中需要至少两台 DHCP 服务器

在大型网络中，需要部署至少两台 DHCP 服务器。如果整个网络中只有 1 台 DHCP 服务器，当这台 DHCP 停止工作时，网络中的工作站可能获取不到 IP 地址，从而引起网络中断。为了提高容错能力，在条件允许的情况下，推荐在网络中部署两台 DHCP 服务器。此时，可以使用 80/20 规则，具体方法是在性能比较好的 DHCP 服务器上，分配约 80%的 IP 地址，在性能一般或者备用 DHCP 服务器上，分配约 20%的 IP 地址，其设置如图 3-1 所示。

如果 DHCP 为多个 VLAN 分配 IP 地址，每个作用域都要按照图 3-1 中的规则进行设置。

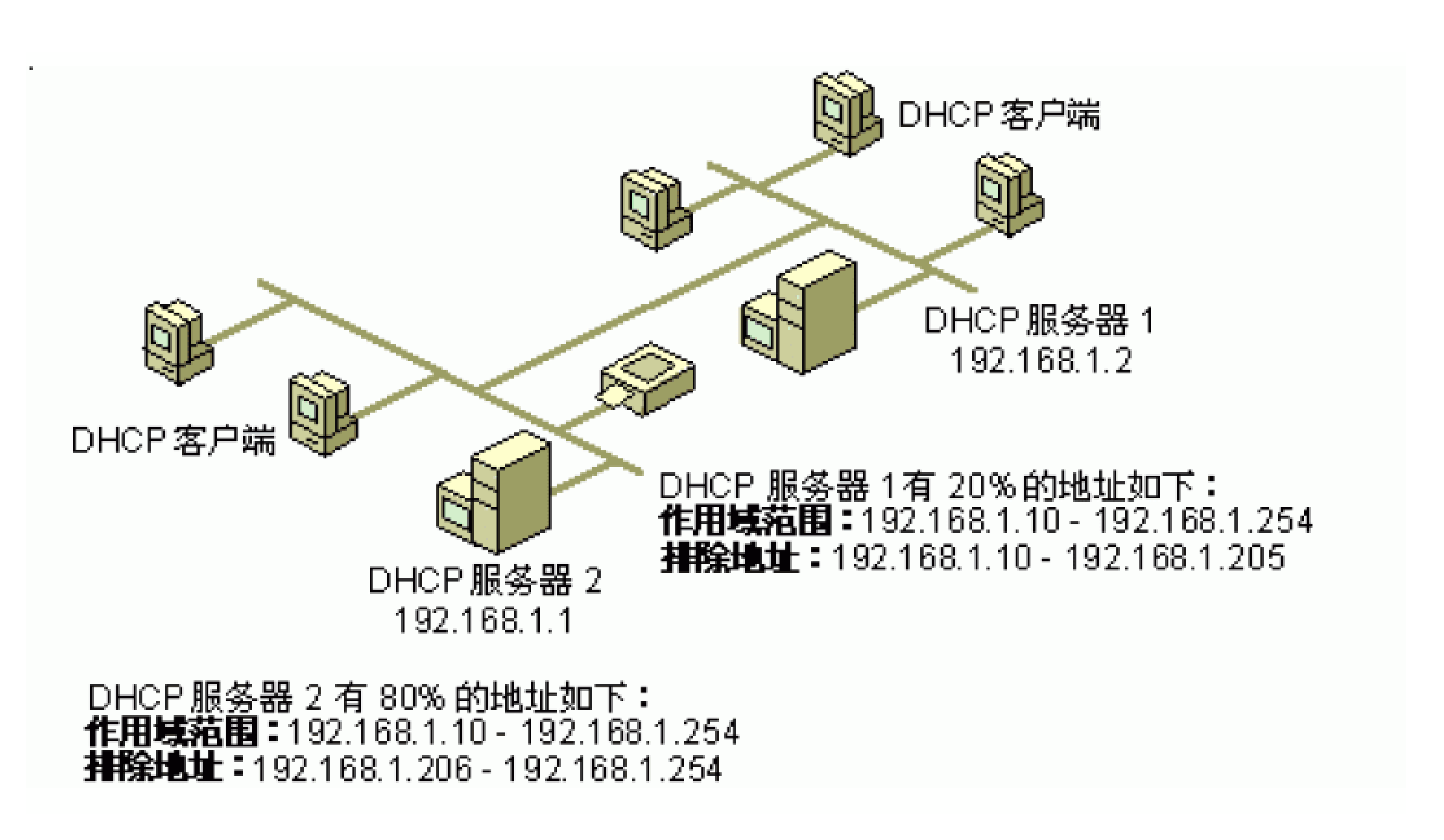
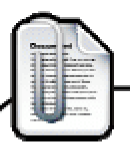


图 3-1　采用 80/20 规则分配 IP 地址



说 明

（1）只有在大型的网络或者重要的网络环境中，才需要部署多台 DHCP 服务器。现在的计算机硬件已经很稳定，在实际生活中，很少有 DHCP 服务器停止工作的例子。所以，在一般情况下，部署一台 DHCP 服务器即可以满足需要。

（2）DHCP 服务器可以采用“硬件”或“服务器”+“DHCP 软件”方式，所谓“硬件”方式，就是某些三层交换机，集成了 DHCP 服务器，例如华为的 53 系列三层交换机。如果是使用交换机集成的 DHCP 服务器，客户端获得地址的方式比较快速，并且工作比较稳定。但集成的 DHCP 服务器，在某些功能上会有限制。

3.1.5　DHCP 服务器授权问题

在 Windows 2000 以前的时代，基于 Windows NT Server 以及其他非 Microsoft 的 DHCP 服务器，只要网络中安装并配置了，网络中的工作站就可以从这些 DHCP 服务器获得地址。如果网络中只有一台 DHCP 服务器，DHCP 工作站可以获得正确的地址。但是，如果网络中有多台 DHCP 服务器（有的 DHCP 服务器并不是网管配置的，也就是说，是一些“非法”的 DHCP 服务器），DHCP 工作站可能会获得不正确的地址从而导致网络通信问题。

基于上述这些问题，在 Windows 2000 Server 中的 DHCP 服务器，引入了“授权”概念，它要求加入到 Active Directory（活动目录服务器）的 DHCP 服务器，必需在 Active Directory 中得到“授权”，只有经过“授权”的 DHCP 服务器才能对外提供服务并对外分配 IP 地址，但是，在 Windows 2000 Server 中，即使 Windows 2000 Server 的 DHCP 服务器并没有加入到 Active Directory，它仍然可以在“未授权”的情况下对外提供服务，所以，对于 Windows 2000 网络来说，这是一点“遗憾”。

而到了 Windows Server 2003 的网络时代，只要网络中存在 Active Directory 服务器，不管 Windows Server 2003 的 DHCP 服务器是否加入到 Active Directory，DHCP 服务器都必需经过“授权”才能工作，这是针对 Windows 2000 网络所做的改进。所以，在 Windows Server 2003 网络中，通常将网络中的 DHCP 服务器作为额外的 Active Directory 服务器。

如果网络中有 Windows Server 2008 的服务器，并且升级到 Active Directory，则网络中的

Windows Server 2003、Windows Server 2008 操作系统的 DHCP 服务器，必需加入到 Active Directory 才能完成“授权”的工作，否则，这些 DHCP 服务器会停止工作，不能提供 IP 地址的分配。

如果你的 Active Directory 服务器不提供 DHCP 服务，无须因为授权而安装 DHCP 服务器组件，只需要安装 Windows Server 2003（或 Windows 2000 Server）管理工具。管理工具可以从 c:\windows\system32\目录下，运行 adminpak.msi 文件包即可（c:\windows 是 Windows Server 2003 的安装目录）。

3.1.6　企业网络中 IP 地址的规划

DHCP 服务器的使用和网络中的 IP 地址规划是分不开的。当网络中的计算机超过一定数量时，就需要划分 VLAN。一般情况下，当计算机数量超过 30 台时，就可以划分多个 VLAN。

在划分 VLAN 的时候，可以根据不同的部门划分，也可以根据不同的楼层划分，这就需要看现有网络中的交换机是否支持。如果中心交换机是一个支持 VLAN 的三层交换机，各楼层的接入交换机是支持 VLAN 的二层交换机，则可以根据部门划分 VLAN；如果各楼层的接入交换机是不支持 VLAN 的普通交换机，则可以按照楼层来划分 VLAN。

在划分 VLAN 的时候，一般采用 10.0.0.0/8、172.16.0.0/16、192.168.0.0/16 的私网地址划分。当划分的网段比较少（100 个以下）时，可以采用 192.168.0.0/16 的网段或 172.16.0.0/16 的网段，只有当网络比较大时，才采用 10.0.0.0/8 的网段。在划分的时候，还要考虑将来的“扩展”需要。

在划分 VLAN 的时候，根据用途不同 “连续”划分。例如：

（1）用于工作站的地址段：192.168.0.0/16～192.168.63.0/16，这样连续有 64 个 C 类地址段，每个地址可以容纳 253 台计算机，一共可以支持 16000 台左右的计算机，能够满足一般企业使用。

（2）用于服务器的地址段：192.168.128.0～192.168.159.0/16，这样连续有 32 个 C 类地址段，每个地址可以容纳 253 台服务器，大约 8000 个地址，能够满足需要。

（3）用于 VPN 客户端的地址：192.168.160.0～192.168.191.0/16,这样连续有 32 个 C 类地址段，足以满足 VPN 客户端访问需要。

（4）用于默认路由的地址：192.168.254.0/16，用于满足交换机“上联”路由器（或者防火墙和代理服务器）的“默认路由”使用，或者连接其他网络，在此有一个 C 类地址段就够了。

（5）在划分 VLAN 的时候，为每个 VLAN 设置一个相同的地址作为网关地址。例如，可以将每个网段的最后一个地址作为网关地址。例如，对于 192.168.0.0/16 的网段，其网关地址是 192.168.0.254。

这样划分的优点如下：

（1）当工作站的地址段不够时，可以继续使用 192.168.64.0～192.168.127.0/16 的地址段；而其他网段（如路由器或代理服务器、VPN 客户端）有需要访问工作站的路由时，只需要添加 192.168.0.0/18（代表 192.168.0.0～192.168.63.0/16）或 192.168.0.0/17（代表 192.168.0.0～192.168.127.0/16）一条静态路由即可。

（2）在其他网段访问服务器时，只需要添加 192.168.128.0/19 一条静态路由即可。

（3）这样划分后，仍然有许多地址可以备用。即使大型的网络，这样划分也能满足需要。

（4）将最后一个地址作为网关地址，1～253 作为可用地址，这样人们在采用“手动方式”设

置 IP 地址时，不容易发生冲突。如果将第 1 个地址作为网关地址，人们在设置 IP 地址时，有可能将第 1 个地址作为工作站的地址，这样容易引起地址冲突。

划分 VLAN 的工作，需要在“中心交换机”以及“接入层交换机”上划分。

当企业网络中有多个 VLAN 时，各个工作站要想接入网络，必需设置正确的 IP 地址、子网掩码、网关、DNS 地址，如果设置了错误的地址，将会引起网络问题。在同一 VLAN 中，如果设置了重复的地址，会造成地址冲突，这些都会给网管员带来负担。此时，可以采用 DHCP 服务器，为网络中的工作站统一、自动分配 IP 地址及其相关参数（如子网掩码、网关、DNS 等）。

3.1.7 VLAN 和 DHCP 中继问题

在划分有 VLAN 的网络中，仍然只需要使用 1 台或 2 台 DHCP 服务器，而不需要在每个 VLAN 中部署一台 DHCP 服务器。在前面已经讲到，DHCP 服务是靠“广播”的方式获得 TCP/IP 地址及其相关参数的，在“屏蔽”广播的 VLAN 之间获得 IP 地址，是靠三层交换机的 DHCP 中继来实现的，在三层交换机中，需要在没有 DHCP 服务器的 VLAN 中，启用并配置 DHCP 中继功能并指定网络中 DHCP 服务器的位置（即 DHCP 服务器的 IP 地址）。

对于 DHCP 服务器来说，无须过多其他的设置，只需要为每个 VLAN 创建一个作用域并正确设置作用域的参数、网关地址及其他参数（如 DNS 地址、WINS 服务器地址）即可。

Windows 2000 Server 和 Windows Server 2003、Windows Server 2008 也提供了“DHCP 中继”功能，但这一项在实际使用中没有多大意义，因为使用三层交换机的成本已经很低，用户无须因为降低成本而使用普通交换机+Windows Server 2003“软路由”的方式划分 VLAN。并且，即使使用 Windows Server 2003 做“DHCP 中继”，但在每个 VLAN 放置一台计算机也是不现实的。在实际的应用中，Windows Server 2003 中的“DHCP 中继”，是为了兼做“路由和远程访问”服务器时，让远程客户端访问内网而使用的，这时候的“DHCP 中继”有其存在的意义。

3.2 DHCP 服务器的安装和使用

如果正在组建一个新的网络，可参考“3.1.6 企业网络中 IP 地址的规划”的方式，为企业网络中的工作站、服务器、VPN（如果存在）、默认路由等进行规划。如果网络已经组建并规划好，需要记住网络中的规划，这包括网络中各 VLAN 的地址段、子网掩码、网关、DNS 等。如果要在网络中配置 DHCP 服务器，需要将 DHCP 和网络中的其他服务器在同一网段，并且在“核心交换机”（通常为三层交换机）指定“DHCP 中继”的地址为网络中 DHCP 服务器的 IP 地址。当交换机的型号不同时，配置方法可能不太相同。如果网络中只有一个网段，或者交换机是普通的交换机，则不需要在交换机中配置 DHCP 中继。下面通过图 3-2 的网络拓扑，介绍网络中 IP 地址、DHCP 服务器的配置。

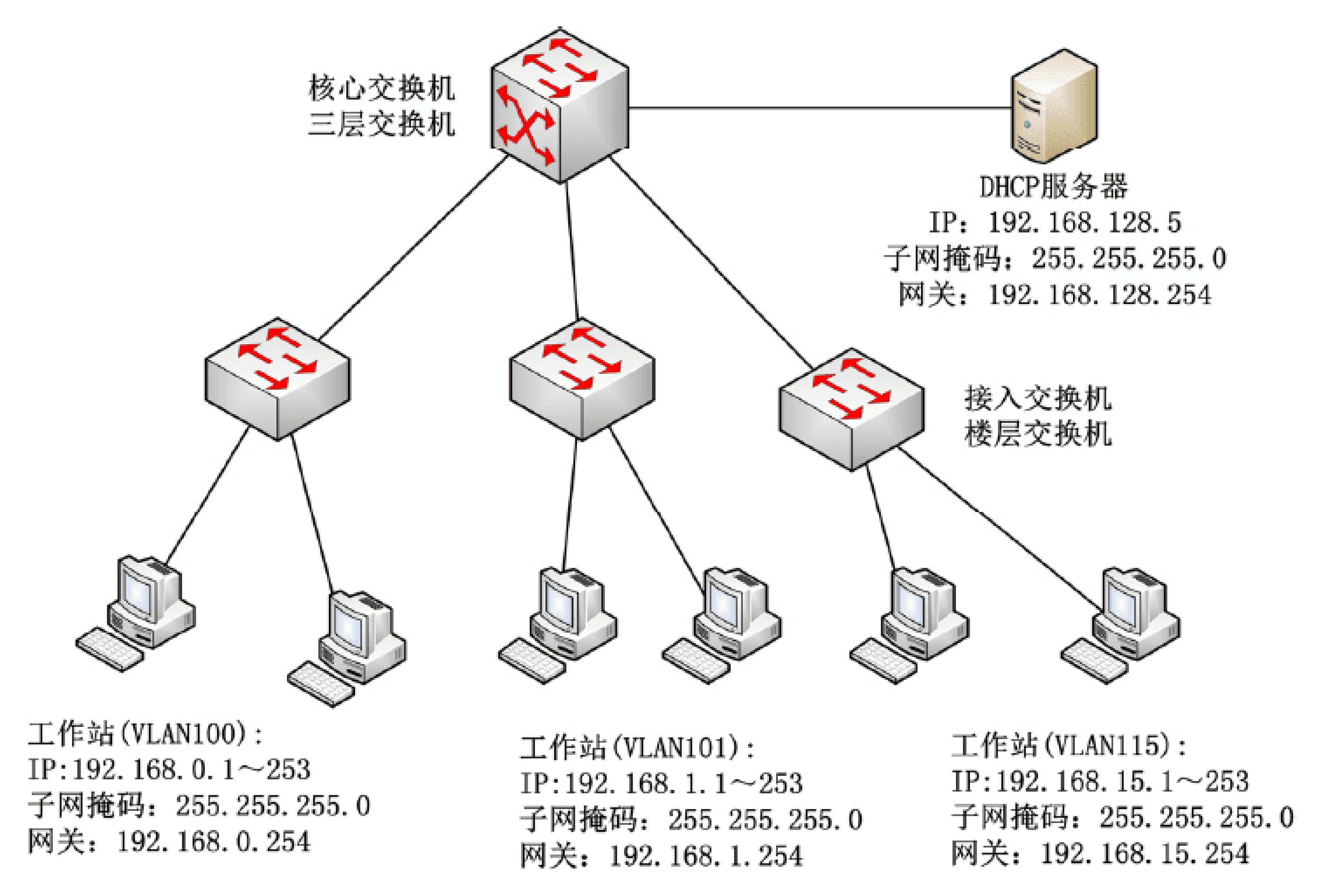


图 3-2　DHCP 配置网络拓扑

在图 3-2 中，工作站使用了 192.168.0.0/24～192.168.0.15/24 共 16 个 VLAN，每个网段的网关地址是最后一个地址。例如，第 1 个工作站网段 VLAN100 的网关地址是 192.168.0.254，网络中的服务器使用了 VLAN128。在本例中，规定 DHCP 服务器的 IP 地址是 192.168.128.5，网关为 192.168.128.254。该 DHCP 服务器，为网络中的所有工作站分配 IP 地址。

3.2.1　DHCP 服务器的安装

本小节将以图 3-2 内容为例，介绍在 Windows Server 2008 R2 中，安装配置 DHCP 服务器的步骤，Windows Server 2008 的 DHCP 服务器与此类似。

01 首先，设置 IP 地址为 192.168.128.5、子网掩码为 255.255.255.0、网关为 192.168.128.254、DNS 为 192.168.128.5，如图 3-3 所示。

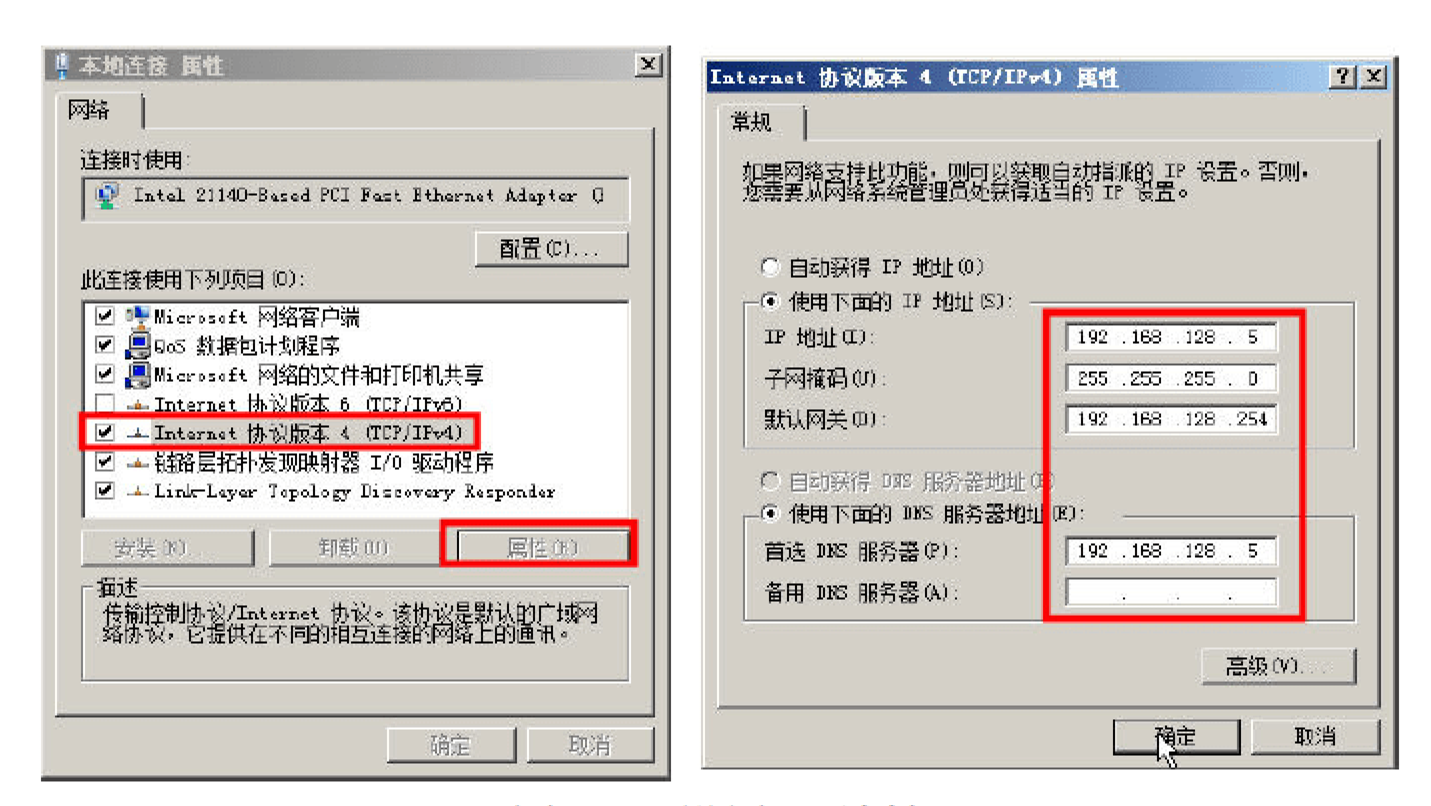


图 3-3　设置 IP 地址

02 然后进入“服务器管理器”窗口，右击“角色”，在弹出的快捷菜单中选择“添加角色”，或者在右侧的“角色”中单击“添加角色”链接，如图 3-4 所示。

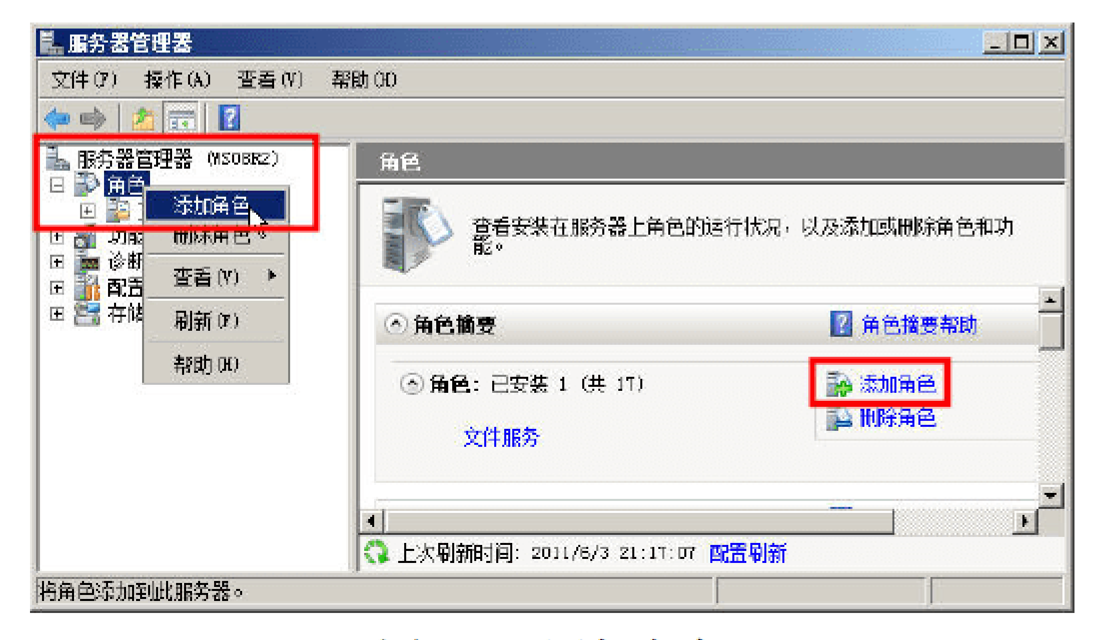
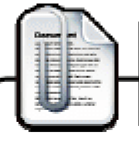


图 3-4　添加角色



说 明

通常情况下，新添加的角色和功能，都是从图 3-4 所示窗口右侧的“添加角色”链接中进入。这相当于以前 Windows Server 2003 中的“控制面板→添加或删除程序→添加/删除 Windows 组件”的链接。

03 在“选择服务器角色”对话框中，选择要安装的角色。在这个对话框中，还可以添加（或删除）Rights Management Services 服务、证书服务、DHCP 服务器、DNS 服务器、IIS、UDDI 服务、Windows 部署服务、传真服务器、打印服务、网络策略和访问服务、终端服务等。在本例中，选择添加 DHCP 服务器，如图 3-5 所示。

04 在“DHCP 服务器”对话框中，显示了 DHCP 服务器的概述及安装注意事项，查看之后，单击“下一步”按钮，如图 3-6 所示。

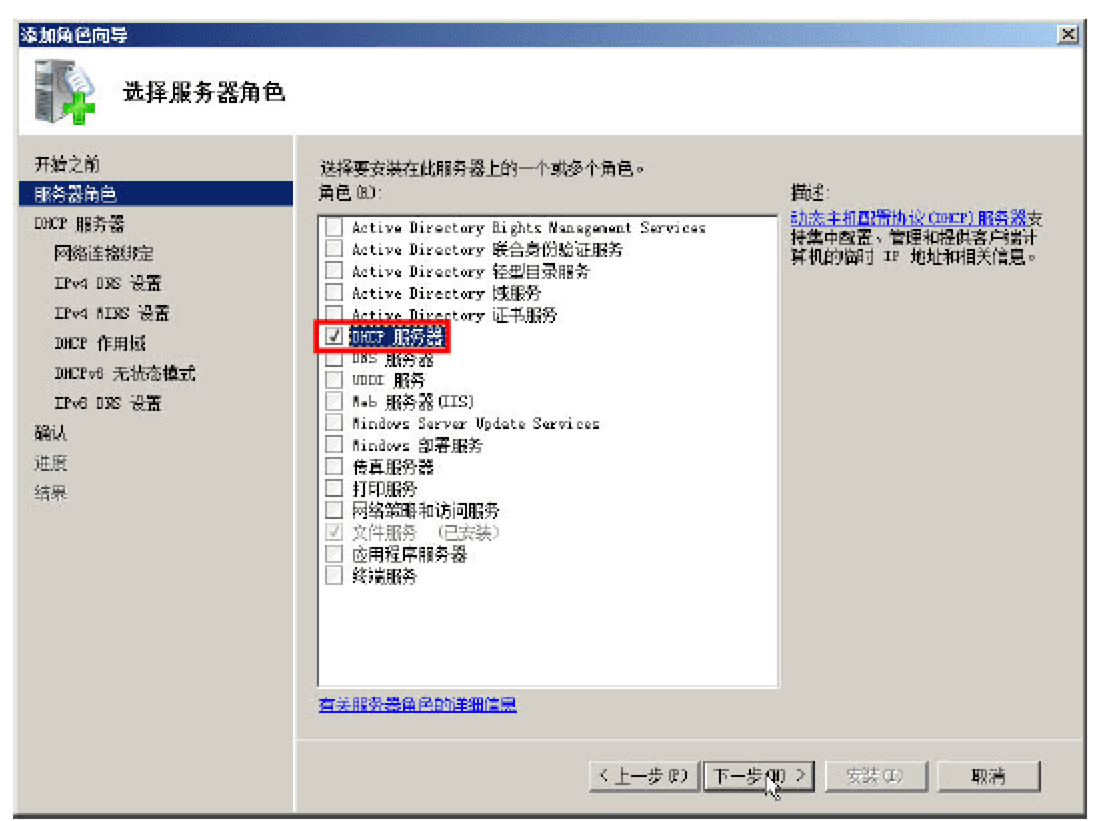


图 3-5　添加 DHCP 服务器

图 3-6　DHCP 服务器简介

05 在“选择网络连接绑定”对话框中，选择向客户端提供服务的网络连接（即侦听 DHCP 客户端请求的网卡及 IP 地址），在此选择 192.168.128.5，如图 3-7 所示。

06 在“指定 IPv4 DNS 服务器设置”对话框中，设置 DNS 服务器的地址。如果当前的计算机“兼做”DNS 服务器，则填写当前的 IP 地址；如果使用 ISP 提供的 DNS 地址，则填写 ISP 的 DNS 地址，如图 3-8 所示。在本例中，设置“父域”域名为“msft.com”、DNS 地址为 192.168.128.5。

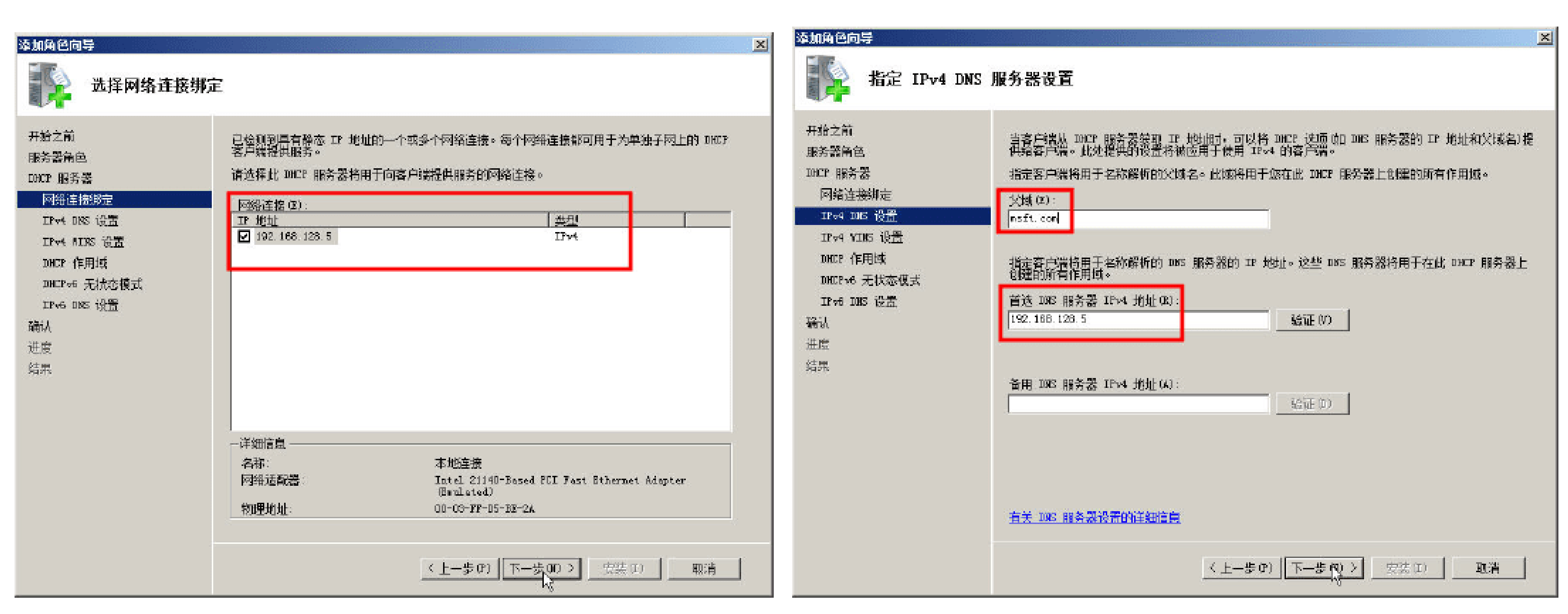


图 3-7　DHCP 服务器地址　　　　图 3-8　DNS 服务器设置

07 在“指定 IPv4 WINS 服务器设置”对话框中，设置当前网络是否需要 WINS 服务器。在此选择“此网络上的应用程序需要 WINS”，并指定 WINS 服务器的地址为当前服务器的地址 192.168.128.5，如图 3-9 所示。

08 在“添加或编辑 DHCP 作用域”对话框，添加作用域的名称、地址范围、子网掩码及网关。在此，根据前面的案例的规划，添加多个 DHCP 作用域。首先单击“添加”按钮，在弹出的“添加作用域”对话框中，输入第一个要添加的作用域的名称及相关参数。在本例中，作用域名称为 VLAN100，起始 IP 地址为 192.168.0.1，结束 IP 地址为 192.168.0.253，子网掩码为 255.255.255.0，默认网关为 192.168.0.254，添加之后单击“确定”按钮，如图 3-10 所示。

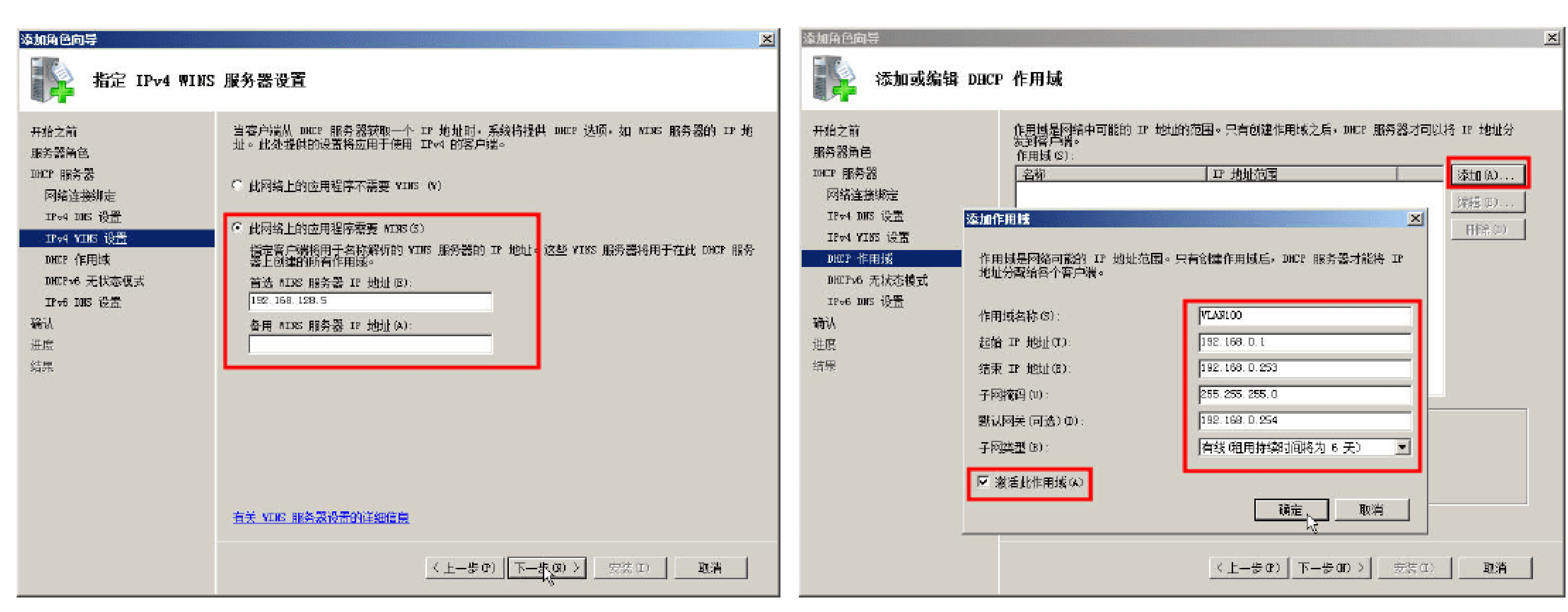


图 3-9　指定 WINS 服务器地址　　　　图 3-10　添加作用域

同样地，添加其他作用域。如果添加的作用域需要修改，可以在“作用域”列表中，选中要修改的作用域，单击“编辑”按钮修改。如果要删除不需要的作用域，在选中作用域之后，单击“删除”按钮即可。在本例中，添加了三个作用域，如图 3-11 所示。

09 在“配置 DHCPv6 无状态模式”对话框中，选择“对此服务器启用 DHCPv6 无状态模式”，如图 3-12 所示。

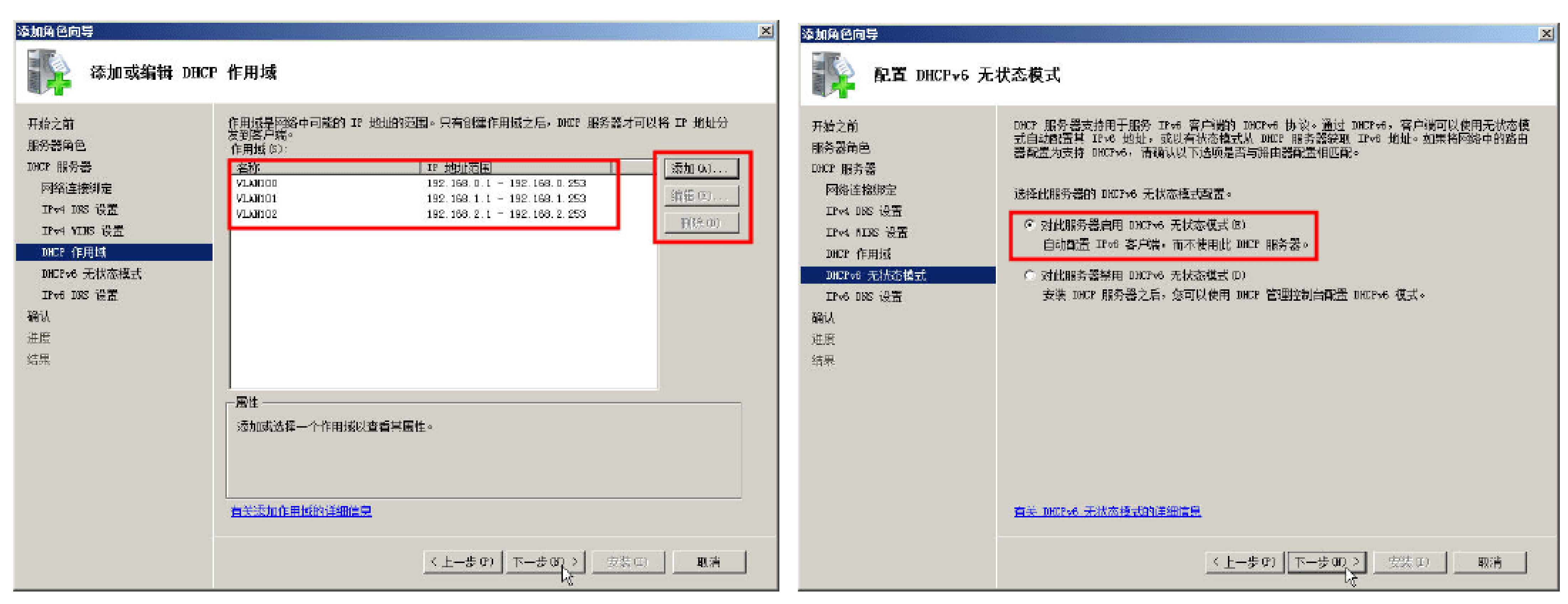


图 3-11　添加三个作用域　　　　图 3-12　DHCPv6 无状态模式

10 在“指定 IPv6 DNS 服务器设置”对话框中，单击“下一步”按钮，如图 3-13 所示。

11 在“确认安装选择”对话框中，显示了要安装的 DHCP 服务器的配置，确认无误之后，单击“安装”按钮，开始安装，如图 3-14 所示。

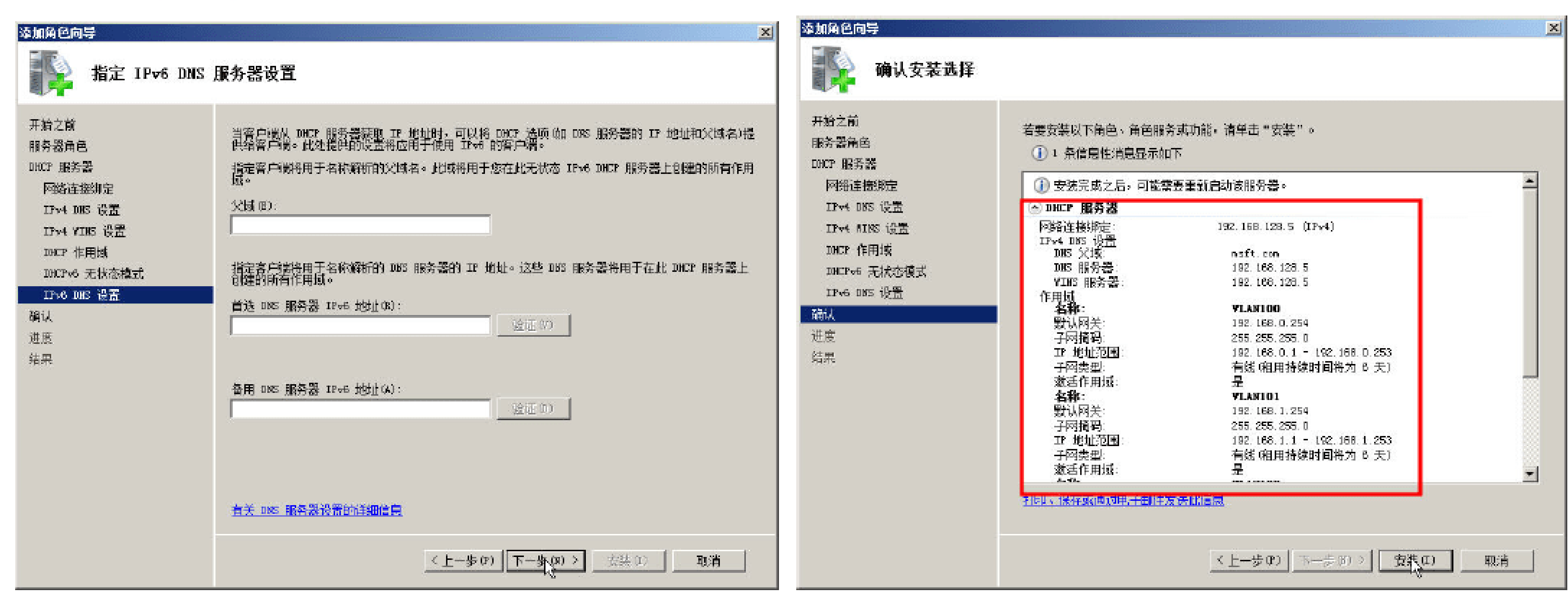


图 3-13　IPv6DNS 服务器　　　　图 3-14　安装选择

12 安装完成之后，在“安装结果”对话框中，显示“安装成功”，如图 3-15 所示，单击“关闭”按钮，完成 DHCP 服务器的安装。

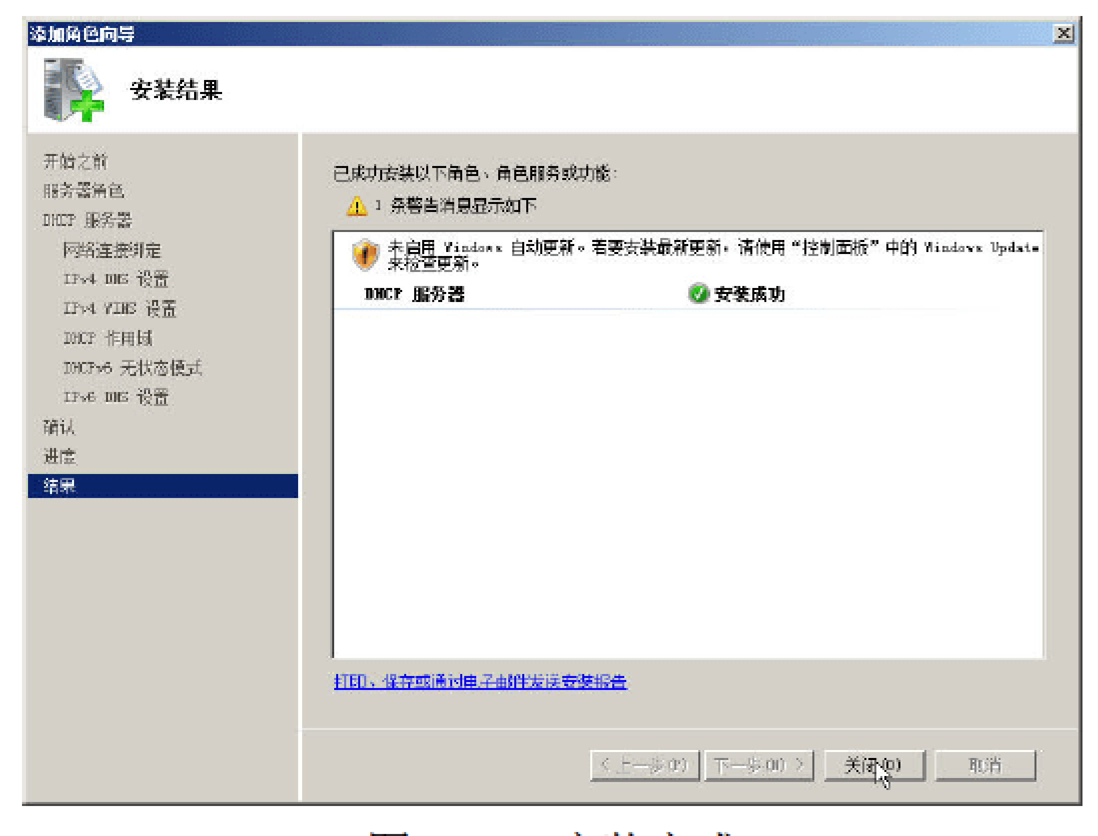


图 3-15　安装完成

3.2.2　在 DHCP 服务器中创建作用域

除了可以在安装 DHCP 服务器的过程中，创建作用域，也可以在安装 DHCP 服务器之后，创建作用域。操作步骤如下。

01 在“服务器管理器”中，定位到“角色→DHCP 服务器→（服务器计算机名称）→IPv4”，右击 IPv4，在弹出的快捷菜单中选择“新建作用域”，如图 3-16 所示。

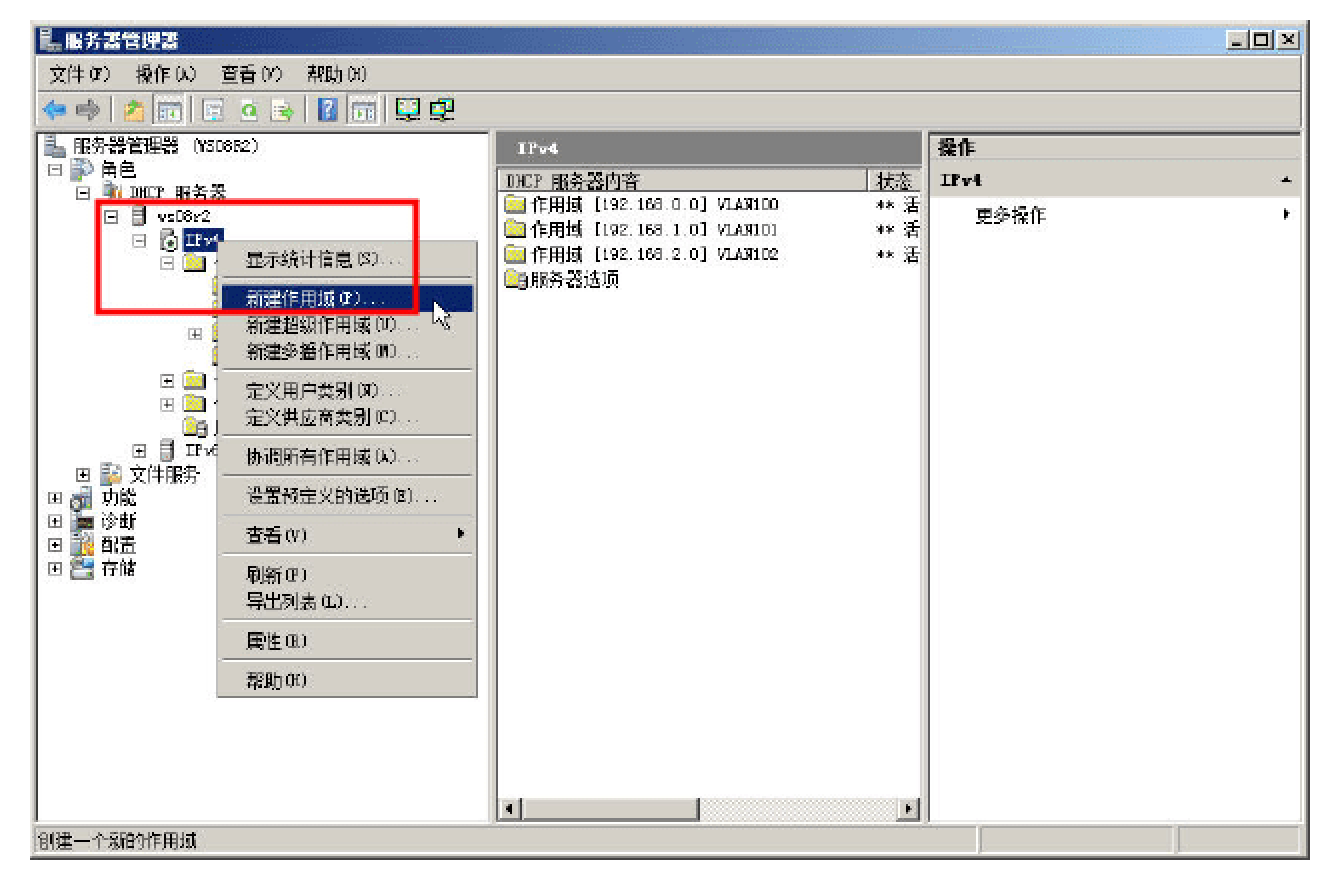


图 3-16　新建作用域

02 在“作用域名称”文本框中输入“VLAN103”，如图 3-17 所示。也可以在“描述”文本框中，输入该作用域的描述信息。

03 在“IP 地址范围”对话框，在“起始 IP 地址”文本框中输入 192.168.3.1，在“结束 IP 地址”文本框中输入 192.168.3.253，在“长度”文本框中输入 24，此时“子网掩码”文本框的数值是“255.255.255.0”，如图 3-18 所示。

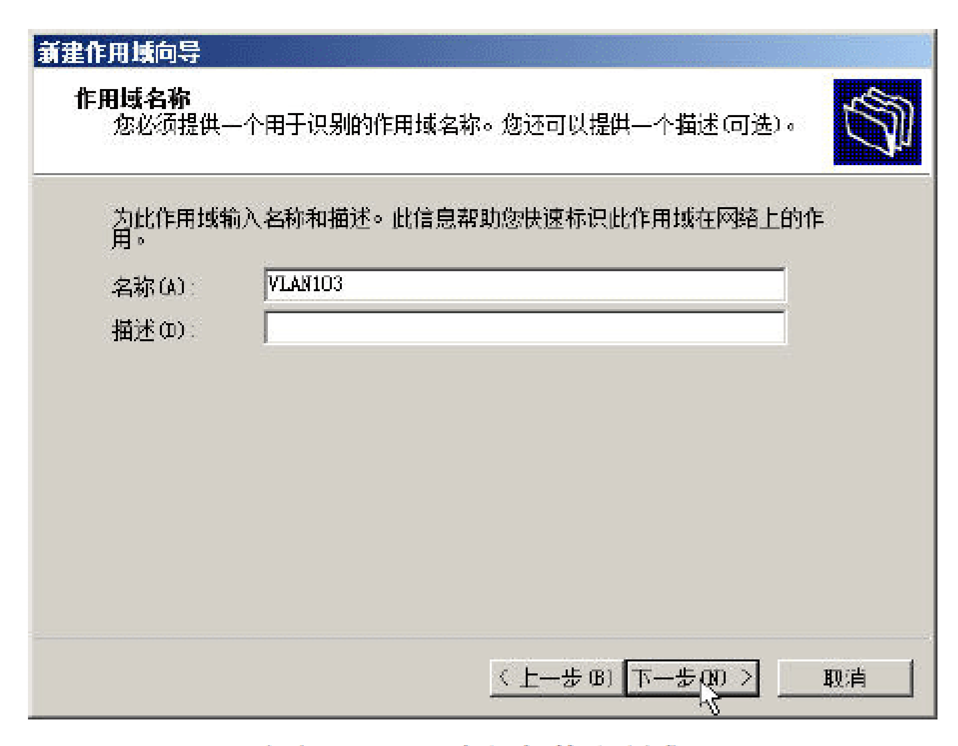


图 3-17　创建作用域

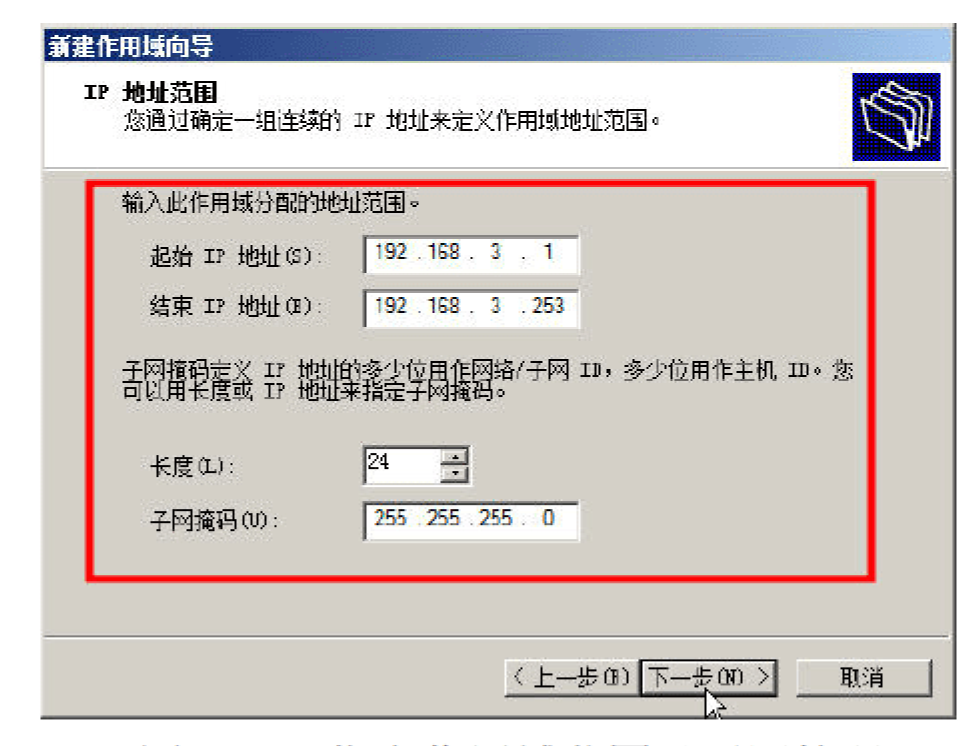


图 3-18　指定作用域范围及子网掩码

04 打开“添加排除”对话框，在“起始 IP 地址”和“结束 IP 地址”文本框中输入将要保留的 IP 地址，在此添加 192.168.3.1 ~ 192.168.3.10 的地址，如图 3-19 所示。可以在此添加多个排除的地址，排除的地址在此 DHCP 服务器将不会用于分配（如果有多个 DHCP 服务器，可以在此 DHCP 服务器添加其他 DHCP 服务器要用于分配的 IP 地址，反之亦然）。

05 打开“租约期限”对话框，设置此作用域的租约期限，默认情况下是 8 天。可以根据需要进行设置，如果用户的网络经常更改 IP 参数，那么可以将此值设置得小一些。如果此作用域用于拨号网络，那么设置得更短，如 30 分钟，通常选择默认值即可，单击“下一步”按钮。

06 打开“配置 DHCP 选项”对话框，选择“是，我想现在配置这些选项”单选按钮，然后单击“下一步”按钮。

07 打开“路由器（默认网关）”对话框，在“IP 地址”文本框中输入当前子网的网关地址 192.168.3.254，单击“添加”按钮，将其添加到下面的列表框中，如图 3-20 所示。

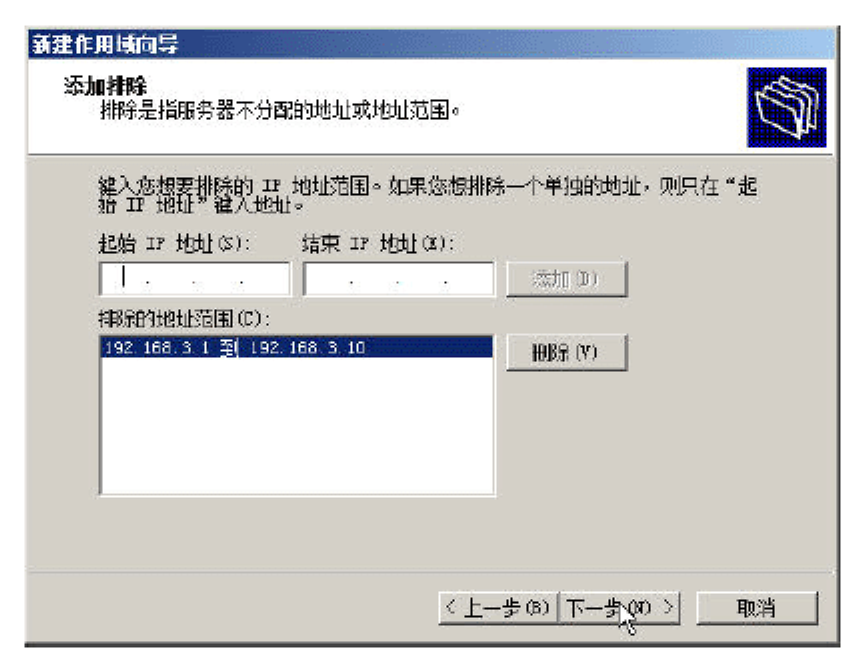


图 3-19　添加排除地址

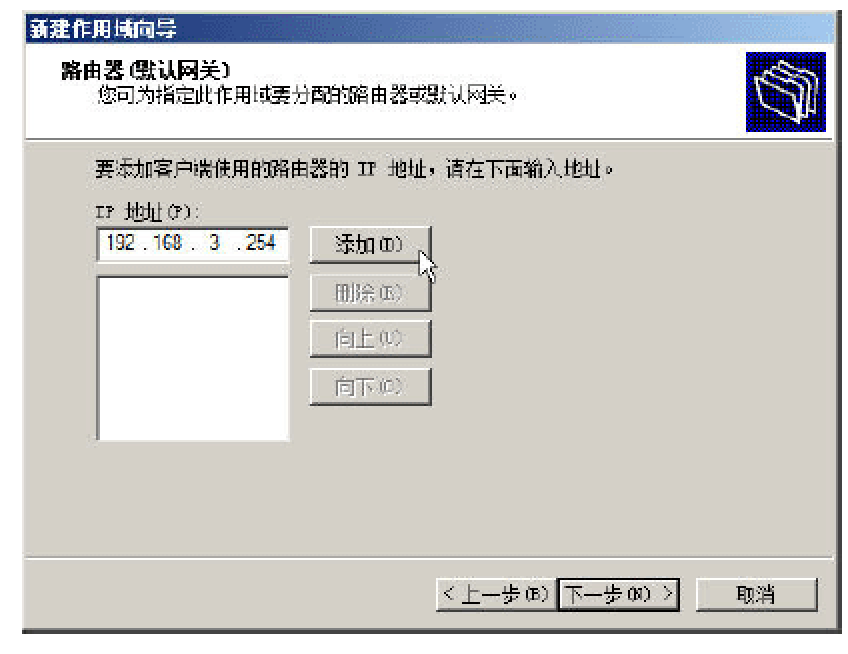


图 3-20　添加网关地址

08 打开“域名称和 DNS 服务器”对话框，在此可添加当前作用域的 DNS 名称和域名。由于此步中的 DNS 名称和下一步中的 WINS 服务器，通常是在 DHCP 服务器的“服务器选项”中设置，所以这里直接单击“下一步”按钮。

09 在以后的步骤中，一直单击“下一步”按钮，在“激活作用域”对话框中选择“是，我想现在激活此作用域”选项，然后在下一个对话框中单击“完成”按钮即可。

其他 VLAN 的作用域创建方法，也可以参照以上步骤进行。

3.2.3　为交换机指定 DHCP 服务器的地址

如果 DHCP 服务器为多个 VLAN 分配 IP 地址（及其他参数），需要配置网络中的三层交换机，启用 DHCP 中继并指定 DHCP 服务器的地址。下面是华为系列交换机启用 DHCP 中继的配置，其中 DHCP 服务器的 IP 地址为 192.168.128.5。华为 8505 的配置如下（其他交换机的配置，读者可以查阅相关的技术文档）：

```
<8505B>sys
Enter system view , return user view with Ctrl+Z.
[8505B]disp curr
#
 sysname 8505B
#
#
 dhcp-server 5 ip 192.168.128.5
 dhcp-server detect
#

interface Vlan-interface100
```

```
 ip address 192.168.0.254 255.255.255.0
 dhcp-server 5
#
interface Vlan-interface101
 ip address 192.168.1.254 255.255.255.0
 dhcp-server 5
#
interface Vlan-interface102
 ip address 192.168.2.254    255.255.255.0
 dhcp-server 5
#
```

3.2.4　配置 DHCP 服务器选项

一台工作站要想正常地访问网络，除了 IP 地址、子网掩码、网关地址外，还需要一些“公共”的信息，如用来解析域名的 DNS 服务器、用来解析 NetBIOS 名称的 WINS 服务器等。虽然可以在配置作用域的时候，为每个作用域指定 DNS 和 WINS 服务器，但这样是比较麻烦的。因为 DNS 服务器和 WINS 服务器对于每个作用域来说都是“相同”的，所以，这可以在“DHCP 服务器选项”中统一配置。

下面介绍在服务器选项中配置 DNS、WINS 服务器地址的方法和步骤。

01 在 DHCP 服务器中，选取“服务器选项”，单击鼠标右键，从弹出的快捷菜单中选择“配置选项”命令（如图 3-21 所示），打开“服务器选项”对话框。先选取“006 DNS 服务器”复选框，在“IP 地址”文本框中输入本网络中 DNS 服务器的 IP 地址，如 192.168.128.5，单击“添加”按钮，如图 3-22 所示。如果网络中有多个 DNS，可以再次添加。

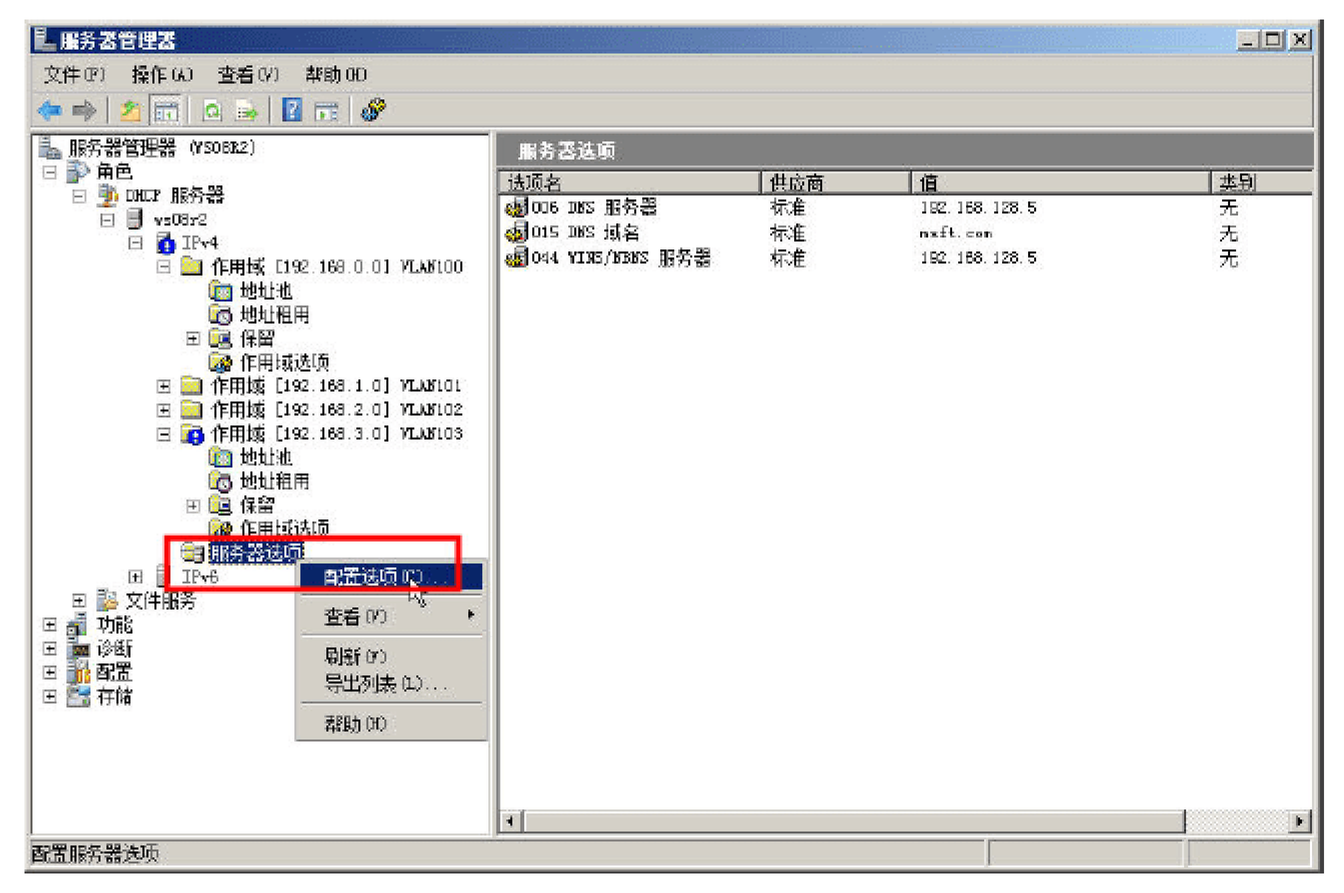



图 3-21　配置服务器选项

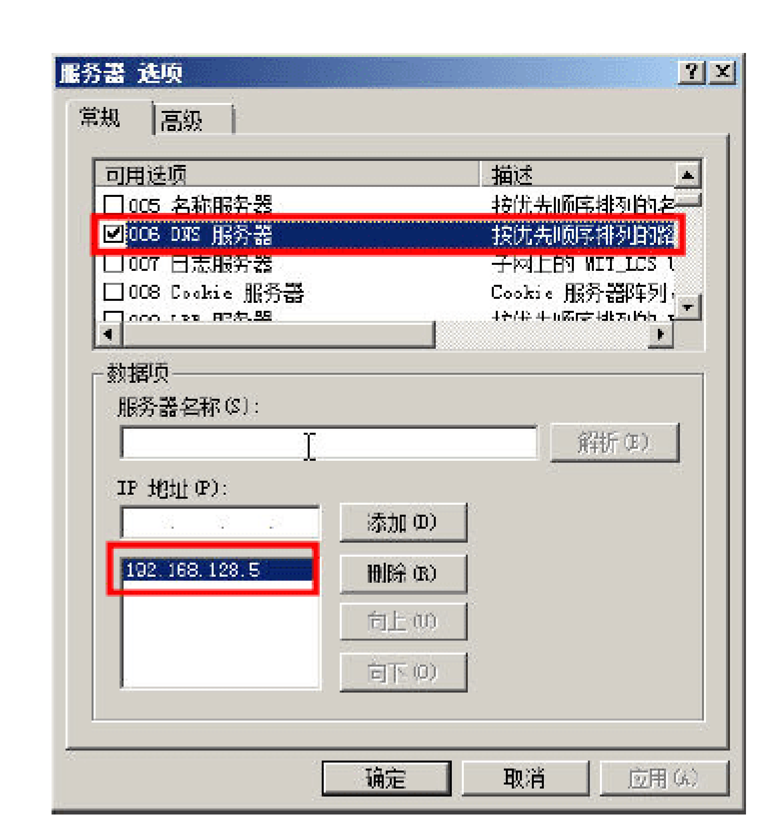


图 3-22　添加 DNS 服务器

可以单击“下移”或者“上移”按钮来调整 DNS 服务器的顺序。

02 选取“044 WINS/BINS 服务器”复选框，添加 WINS 服务器的地址。

03 选取“046 WINS/BINS 节点类型”复选框，并修改节点类型为 0x8。

以后，可以在“服务器选项”对话框中，修改 DNS、WINS 服务器等参数。



说 明

如果同时在作用域选项和服务器选项中配置了相同的参数（如 DNS 服务器），则作用域的选项优先于服务器选项。例如，在服务器选项配置了 DNS 地址为 202.206.192.33，而在某个作用域选项配置了 DNS 地址为 202.99.160.68，则该作用域所有的工作站获得的 DNS 地址将是 202.99.160.68 而不是 202.206.192.33。

3.2.5　创建保留地址

DHCP 服务器为用户分配 IP 地址时，是“先来先获得”的原则，通常情况下，最先从 DHCP 服务器申请 IP 地址的计算机，将从地址池获得比较低的地址，后面的计算机则分配比较高的地址，并且，工作站每次获得的地址可能不尽相同。在许多时候，一些客户机要求获得固定的 IP 地址，这就需要在 DHCP 服务器中，使用创建“保留”地址的方法，为某些客户机分配指定的 IP 地址。

在为客户机分配指定的 IP 地址时，需要事先知道客户机的 MAC 地址，可以在客户机上使用 ipconfig/all 命令获得网卡的 MAC 地址。例如，一台计算机显示如下：

```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
Physical Address. . . . . . . . . : 00-E0-4C-12-34-56
Dhcp Enabled. . . . . . . . . . . : No
IP Address. . . . . . . . . . . . : 192.168.2.3
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

其中“Physical Address”后面的 6 个字节十六进制数字即是该网卡的 MAC 地址。

下面来介绍在 DHCP 服务器为指定 MAC 地址的计算机划分指定 IP 地址的方法（在 DHCP 服务器中称作“添加保留地址”）。本例将为 MAC 地址为“00.E0.4C.12.34.56”的网卡保留 IP 地址 192.168.1.123。

01 进入 DHCP 服务器，在相应的作用域（如想保留 192.168.1.123 的地址，需要在作用域地址范围包括 192.168.1.0 的作用域）定位到“保留”，右击“保留”，从弹出的快捷菜单中选择“新建保留”命令，如图 3-23 所示。

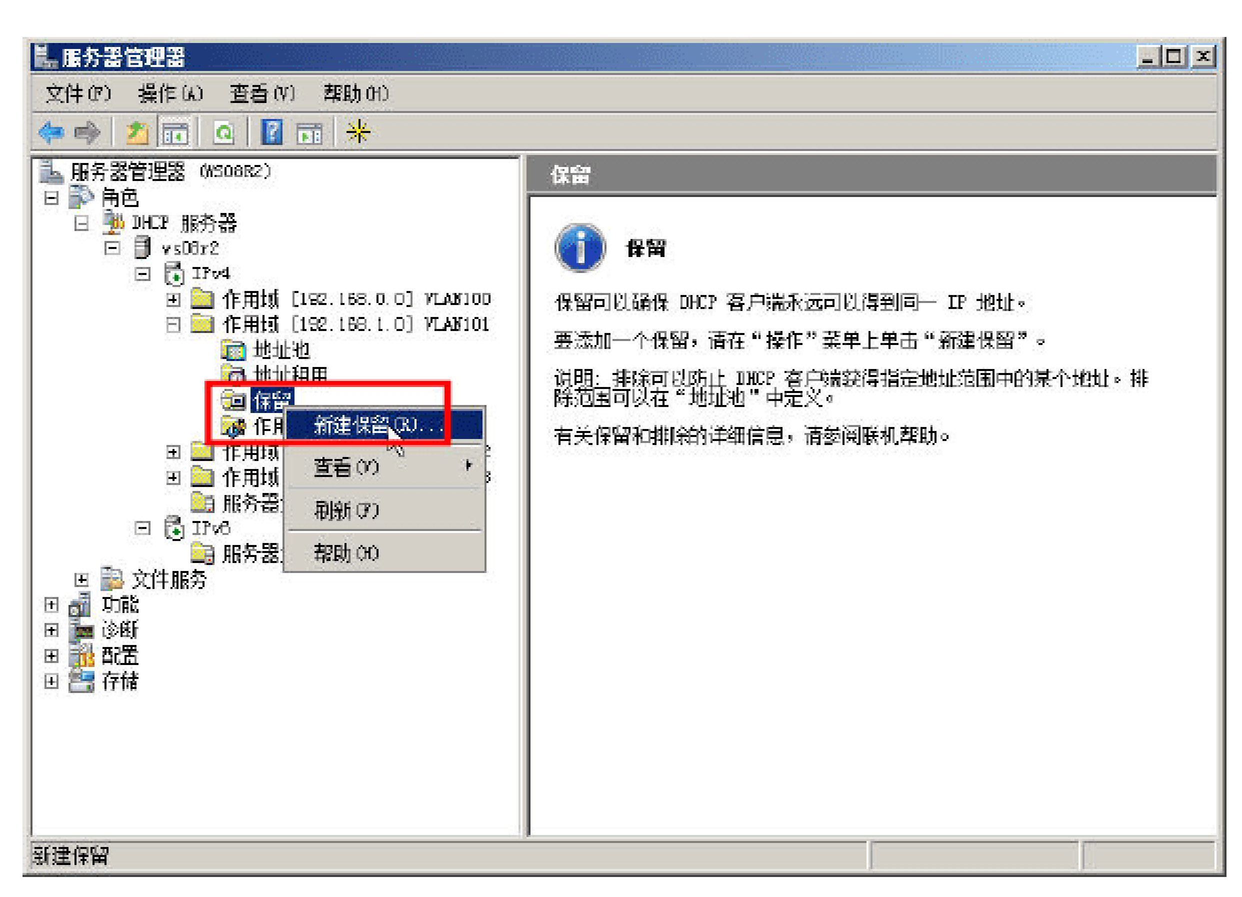


图 3-23　为指定工作站保留 IP 地址

02 打开“新建保留”对话框，在“保留名称”文本框中输入一个标识信息，在“IP 地址”字段后面输入想要保留的 IP 地址，在“MAC 地址”后面输入想要保留此地址的计算机网卡地址（连续输入，中间不要有短横线“-”），然后单击“添加”按钮，如图 3-24 所示。

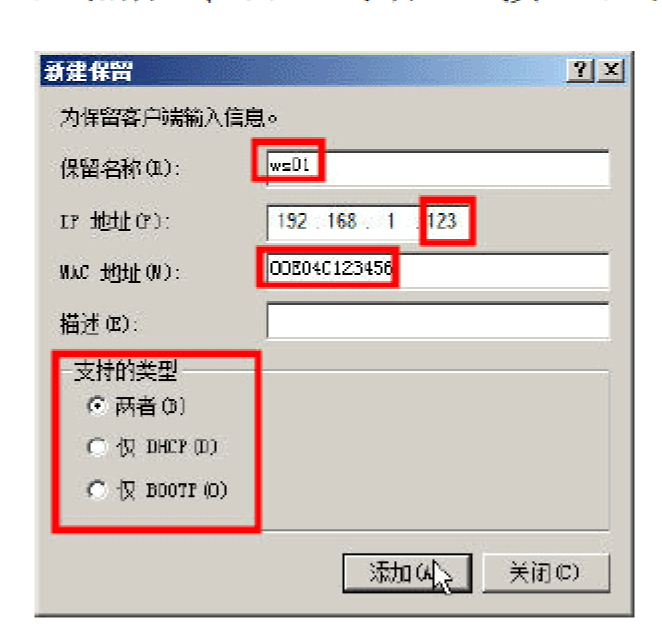


图 3-24 为指定工作站保留 IP 地址

03 如果网络中有多台 DHCP 服务器，则需要在每一台 DHCP 服务器上，都要为保留的地址创建一次。

04 如果有其他计算机需要分配指定的 IP 地址，则参照步骤 1～3 创建。

接下来，我们来看看保留地址的高级用法，初学者可以跳过以下内容。

01 使用 DHCP 服务器为指定的计算机分配指定的 IP 地址，只是一种“软”的方式，如果网络中有其他计算机，手动设置了为用户保留的 IP 地址，则用户仍然不能使用。例如，假设在 DHCP 服务器上为 A 计算机保留了 192.168.5.88 的 IP 地址，但网络上的 B 计算机使用“手动”的方式设置了 192.168.5.88 的 IP 地址并且比 A 计算机早开机，则 A 计算机即使从 DHCP 服务器获得 192.168.5.88 的地址，仍然不能使用。解决此问题的方法很简单，可以在三层交换机中，为指定的 MAC 地址绑定指定的 IP 地址，这样，B 计算机即使手动设置了某个被保留的地址，仍然不能使用。例如，表 3-1 中需要为下列用户保留下面的地址，除了在 DHCP 服务器创建保留地址外，还可以在三层交换机上绑定这些地址。

表 3-1 需要保留 IP 地址的用户列表

部门	人员	房间号	MAC 地址	IP 地址
办公室	张主任	201	00.0B.6A.F7.09.82	192.168.2.10
办公室	李干事	202	00.0B.6A.45.23.46	192.168.2.12
领导	张总	305	00.0B.6A.27.39.21	192.168.3.16
领导	李总	309	00.0B.6A.F7.92.53	192.168.3.18
……	……	……	xx.xx.xx.xx.xx.xx	172.30.xx.xx

在 DHCP 服务器上创建了保留地址后，登录网络中的“中心交换机”，将 MAC 地址和 IP 地址进行绑定。以华为交换机为例：

```
[8505B]arp static   192.168.2.10   000B-6AF7-0982
[8505B]arp static   192.168.2.12   000B-6A45-2346
[8505B]arp static   192.168.3.16   000B-6A27-3921
[8505B]arp static   192.168.3.18   000B-6AF7-9253
```

02 在上述案例中，如果要为所有的用户都绑定 IP 地址，将所有的地址绑定后，还要将网络中“没有使用”的 IP 地址和一空 MAC 地址相绑定，这样就杜绝了非授权的计算机使用网络资源。所谓“没有使用”的 IP 地址，就是在表 3-1 中没有绑定 MAC 地址的 IP 地址，例如，在 VLAN3011 中，地址范围是 192.168.1.1 ~ 192.168.1.254，假定我们使用了 192.168.1.10 ~ 192.168.1.125，网关地址使用的是 192.168.1.254，则需要将 192.168.1.1 ~ 192.168.1.9 和 192.168.1.126 ~ 192.168.1.253 都使用“00.01.00.01.00.01”绑定。在华为交换机上，配置如下：

```
[8505B]arp static 192.168.1.1 0001-0001-0001
[8505B]arp static 192.168.1.2 0001-0001-0001
[8505B]arp static 192.168.1.3 0001-0001-0001
[8505B]arp static 192.168.1.4 0001-0001-0001
……
[8505B]arp static 192.168.1.253 0001-0001-0001
```

3.3　DHCP 服务器的管理

介绍完不同网络环境中 DHCP 服务器的配置后，接下来将讲述 DHCP 服务器的管理和 DHCP 客户端的配置。首先介绍 DHCP 服务器端的管理，这涉及作用域的管理、DHCP 服务器的备份和还原等。

3.3.1 作用域的管理

在 DHCP 服务器中，可以创建和删除作用域，可以暂时停用作用域，也可以在需要的时候激活作用域。

在 DHCP 服务器操作窗口中，选取一个作用域，单击鼠标右键，从弹出的快捷菜单中可以选择相应的功能进行管理，如图 3-25 所示。

如果想停用选取的作用域，从弹出的快捷菜单中选择“停用”命令即可。如果作用域已经被停用，则相应的位置变为“激活”。如果作用域不再使用，可以选择“删除”命令，删除不再使用的作用域。

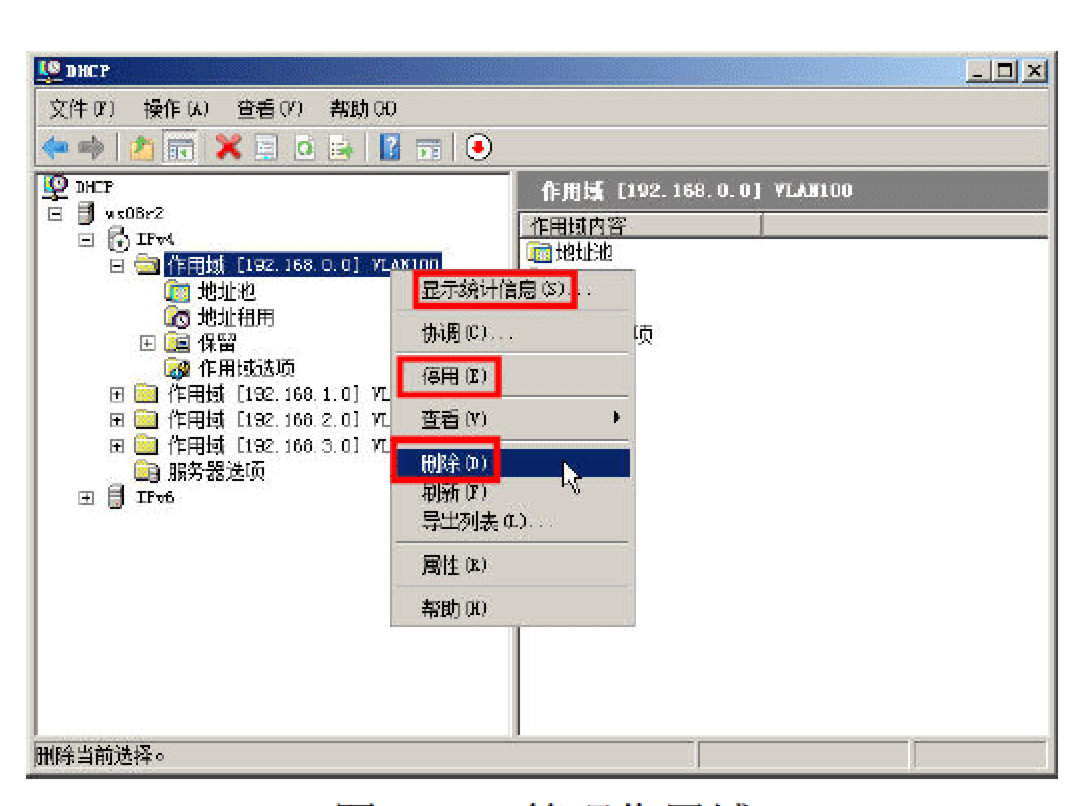


图 3-25　管理作用域

如果选择“显示统计信息”，将显示 DHCP 服务器分配的 IP 地址等情况。

3.3.2　DHCP 服务器的常规管理

在 DHCP 服务器管理窗口中，选取 DHCP 服务器的计算机名称，右击“IPv4”，从弹出的快捷菜单中选择“属性”命令，将打开如图 3-26 所示的 DHCP 服务器属性对话框。

01 在“常规”选项卡中，可以设置统计信息的间隔时间和 DHCP 审核记录等。这里通常选择默认值。

02 打开“DNS”选项卡，如图 3-27 所示。如果网络中的 DHCP 客户端计算机是 Windows 2000 以上，或者没有启用内部的 DNS 服务器，在“DNS”选项卡中，可以选择默认值。如果网络中的 DHCP 客户端计算机有 Windows 98、Windows NT 版本，并且想让这些以前版本的计算机名称在 DNS 中注册，可从图 3-27 中选取“总是动态更新 DNS A 和 PTR 记录”单选按钮和“为不请求更新的 DHCP 客户端动态更新 DNS A 和 PTR 记录”复选框。

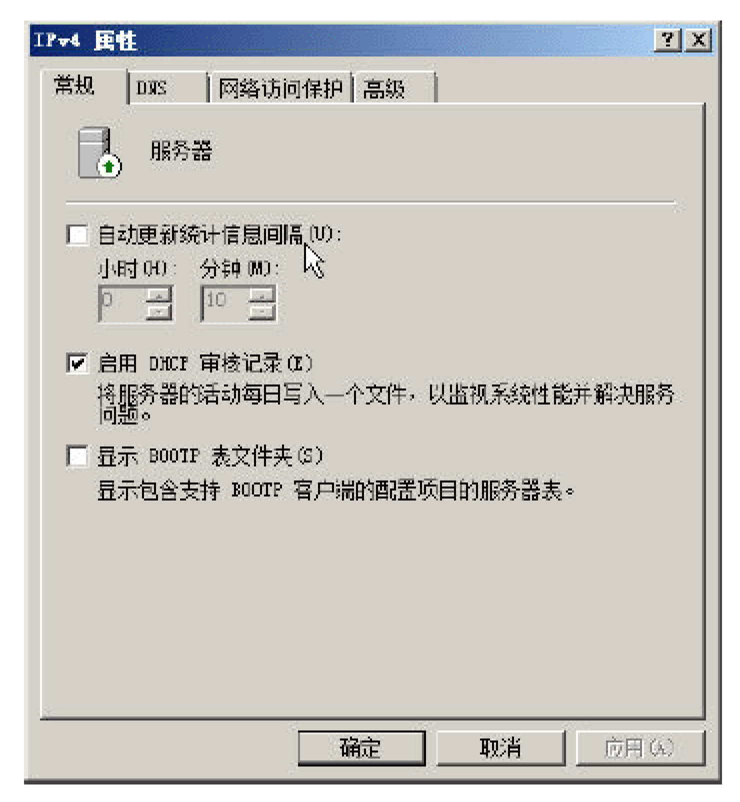


图 3-26　DHCP 常规选项卡

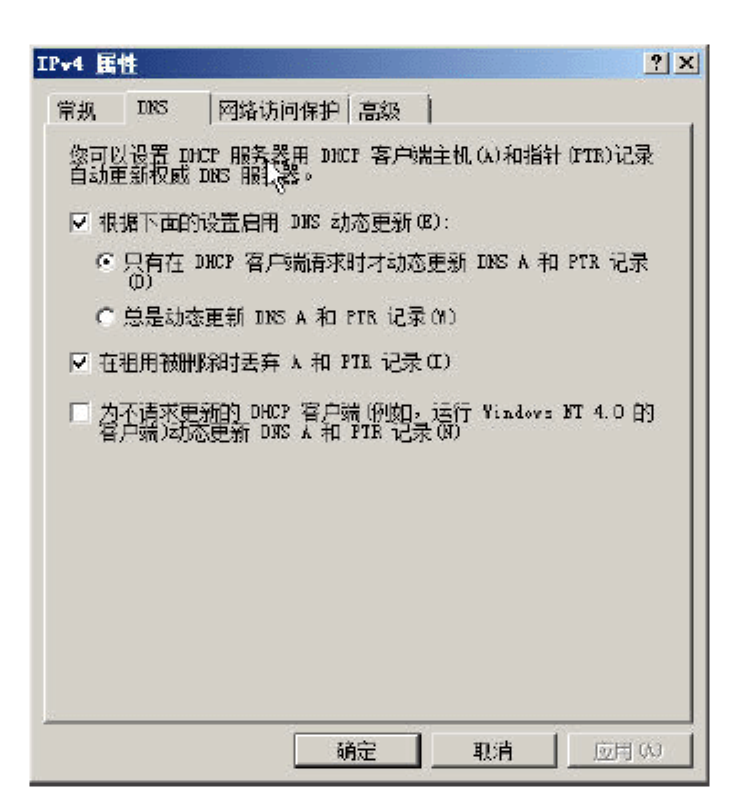


图 3-27　DNS 选项卡

03 在“网络访问保护”选项卡中，选择是否通过 DHCP 服务器强行实施网络访问保护，如图 3-28 所示。

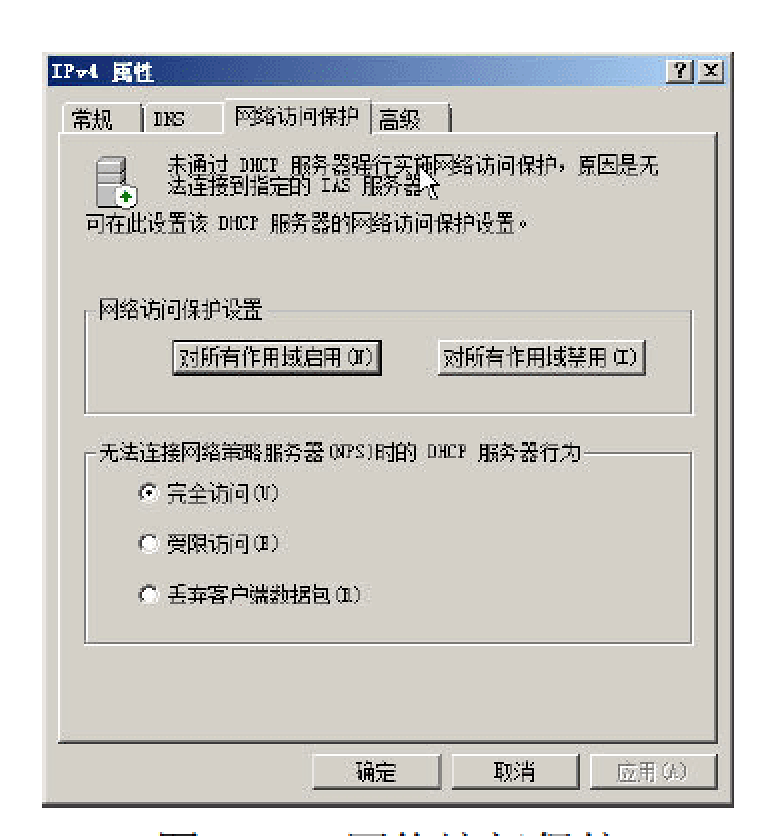


图 3-28　网络访问保护

04 在使用 DHCP 服务器的网络中，如果网络中的计算机有手动设置 IP 地址的，也有自动获

取 IP 地址的，则 DHCP 服务器分配给 DHCP 客户机的地址中，有可能引起冲突。如果存在这种情况，则在“高级”选项卡中的“冲突检测次数”微调框中，设置 0 以外的数字（如 1），如图 3-29 所示。这样 DHCP 服务器在分配地址时，将对分配的地址进行检测。如果网络上已经有计算机使用了该地址，那么 DHCP 服务器将重新为客户端分配一个地址。

如果 DHCP 服务器上使用了多块网卡，可以单击“绑定”按钮，选择 DHCP 服务器为客户端提供服务所使用的网卡，如图 3-29 所示。

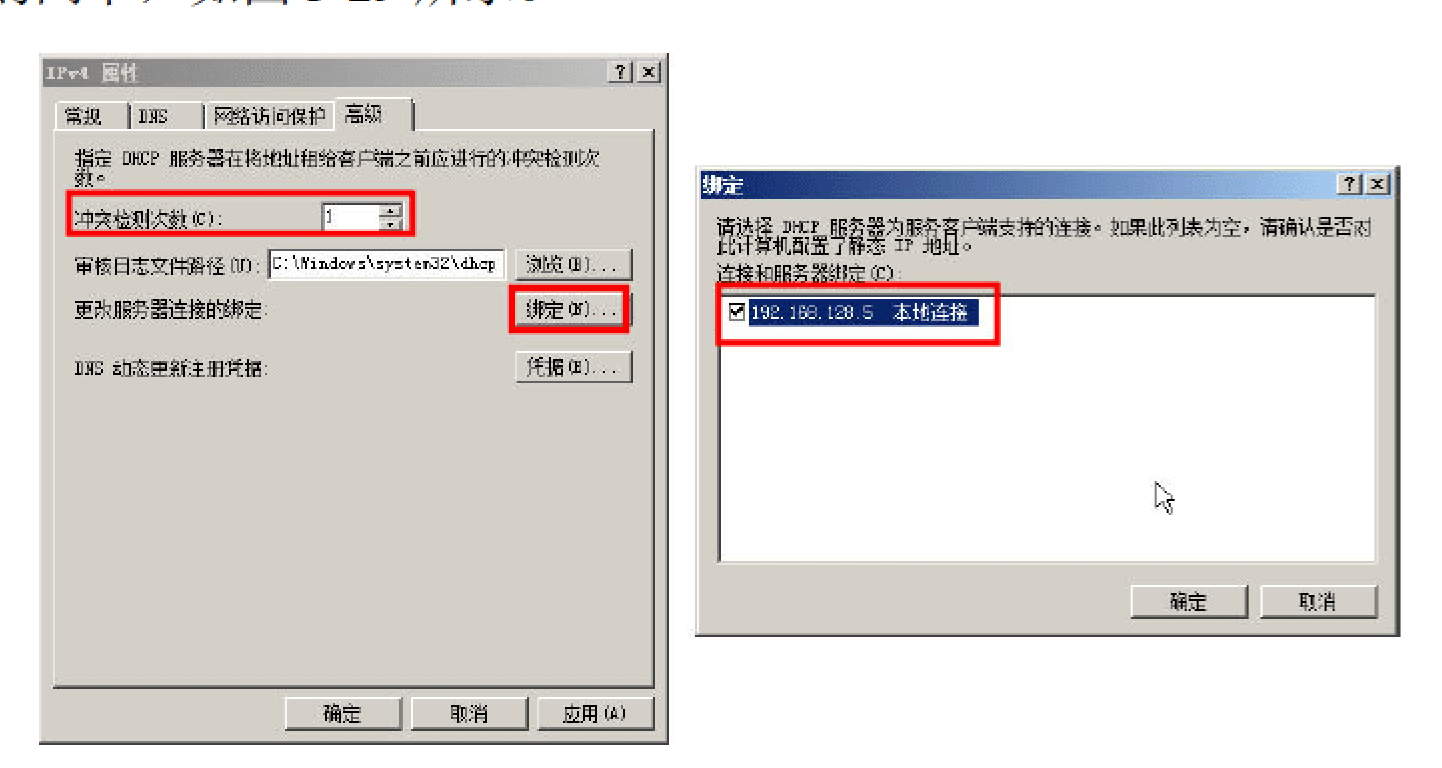


图 3-29　冲突检测和选择 DHCP 服务器为监听的网卡

3.3.3　作用域属性

除了在 DHCP 服务器属性中，对 DHCP 服务器进行统一的配置外，还可以单独对每个作用域进行配置。

01 在 DHCP 服务器中，右击作用域，在弹出的快捷菜单中选择“属性”，如图 3-30 所示。

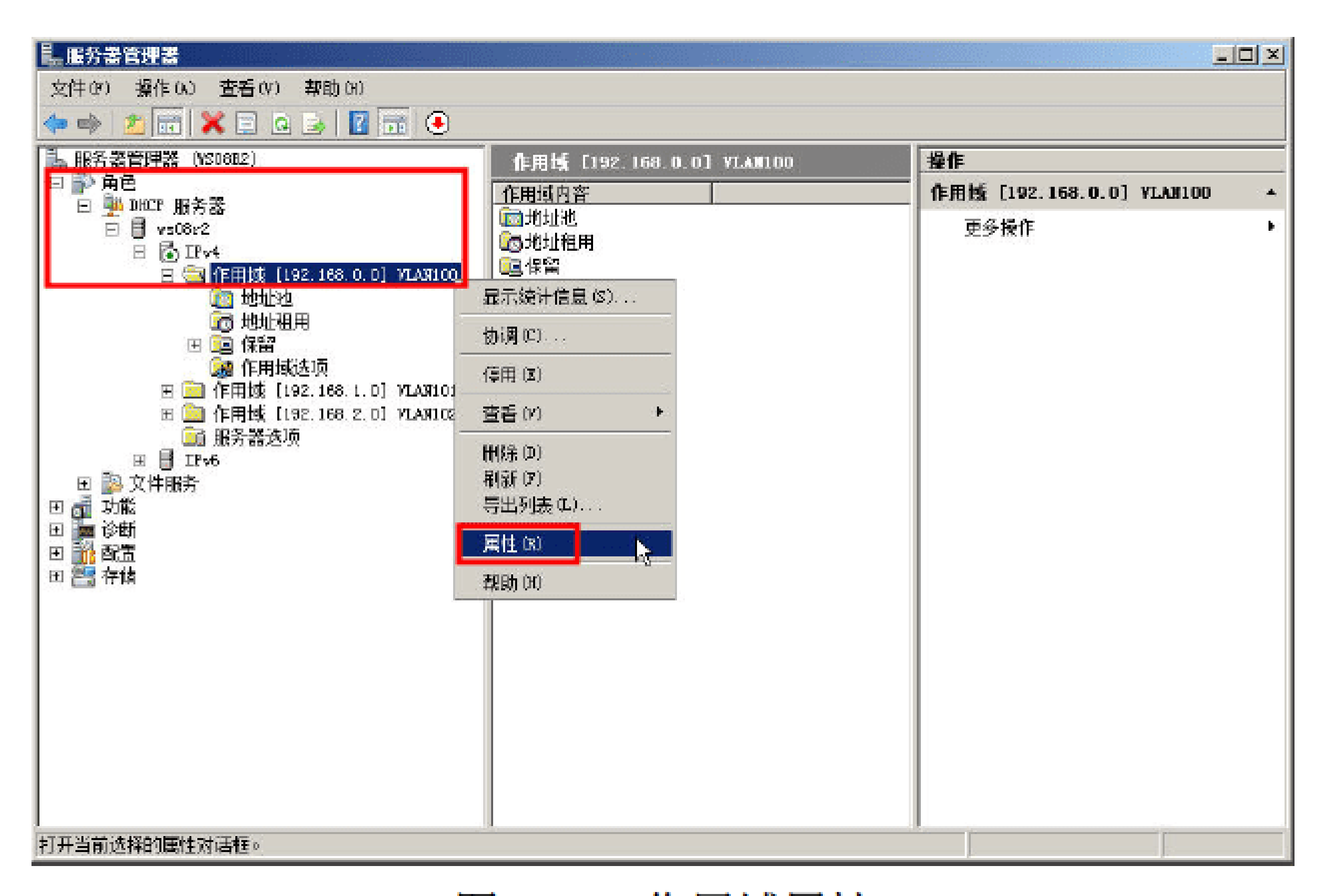


图 3-30　作用域属性

02 在“常规”选项卡中，可以修改作用域的名称、起始和结束 IP 地址、租用期限，如图 3-31 所示。

03 在“高级”选项卡中，可以指定为哪些客户端分配 IP 地址。选中“仅 DHCP”单选按钮，将只能为安装有操作系统（如 Linux、Windows）的计算机或设备分配 IP 地址；选中“仅 BOOTP”

单选按钮将为没有安装操作系统、处于网络启动（如某些无盘工作站的初始启动、Windows 部署服务的初始配置）的计算机或设备分配 IP 地址；选中“两者”单选按钮将为所有设备分配 IP 地址，如图 3-32 所示。

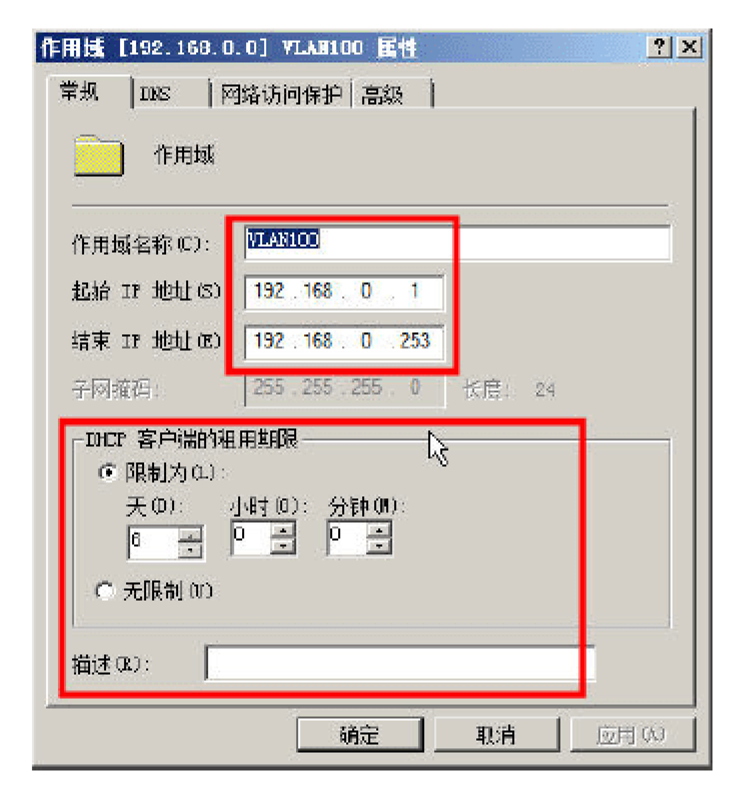


图 3-31　作用域“常规”选项卡

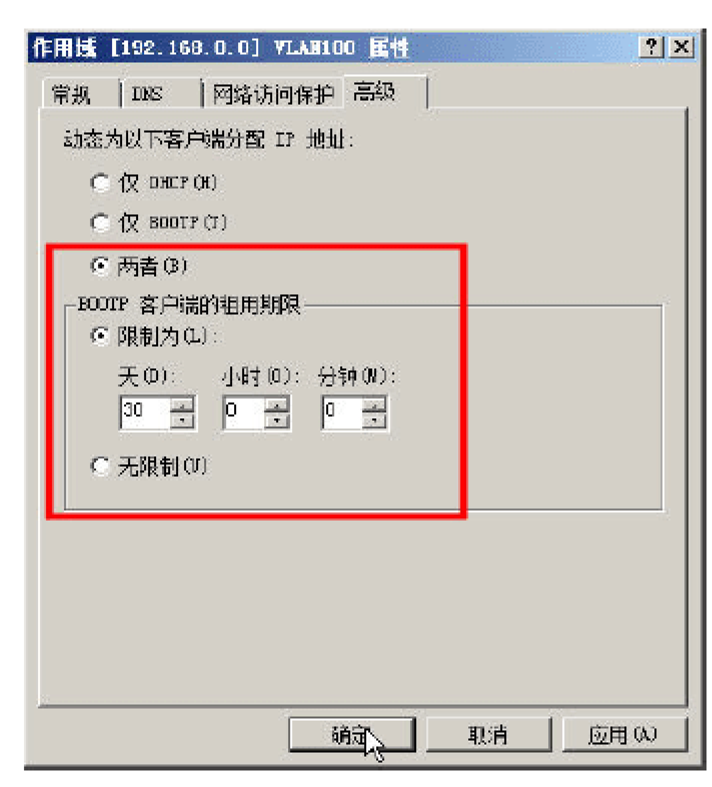


图 3-32　作用域“高级”选项卡

3.3.4　在 Active Directory 中授权

如果网络使用“Active Directory”进行管理，则 DHCP 服务器必需经过“授权”才能工作。在“Active Directory”服务器上对 DHCP 服务器授权的具体步骤如下。

01 在“Active Directory”服务器上，以 Administrator 身份登录。

02 从“管理工具”中运行“DHCP”，打开“DHCP”窗口。

03 在左侧窗格中选取 DHCP，单击鼠标右键，从弹出的快捷菜单中选择“管理授权的服务器”命令（如图 3-33 所示），打开“管理授权的服务器”对话框，单击“授权”按钮，在弹出的“授权 DHCP 服务器”对话框中输入 DHCP 服务器的 IP 地址，在弹出的“确认授权”对话框中，单击“确定”按钮即可。可以对多台 DHCP 服务器进行授权，也可以在此对话框中解除对某台 DHCP 服务器的授权，如图 3-34 所示。

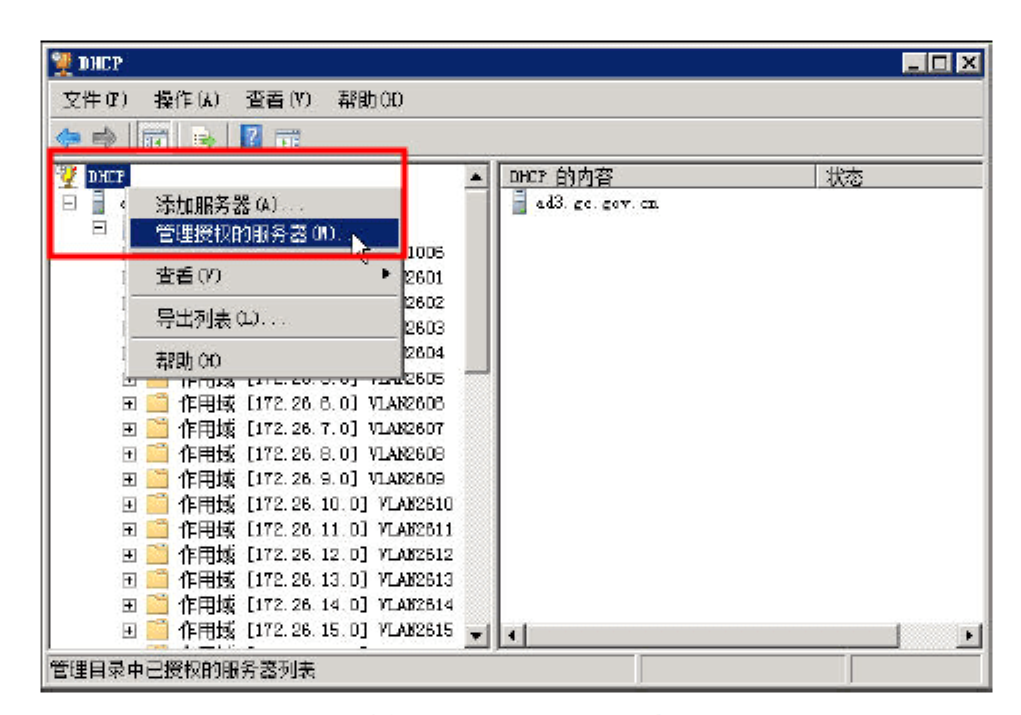


图 3-33　管理授权的服务器

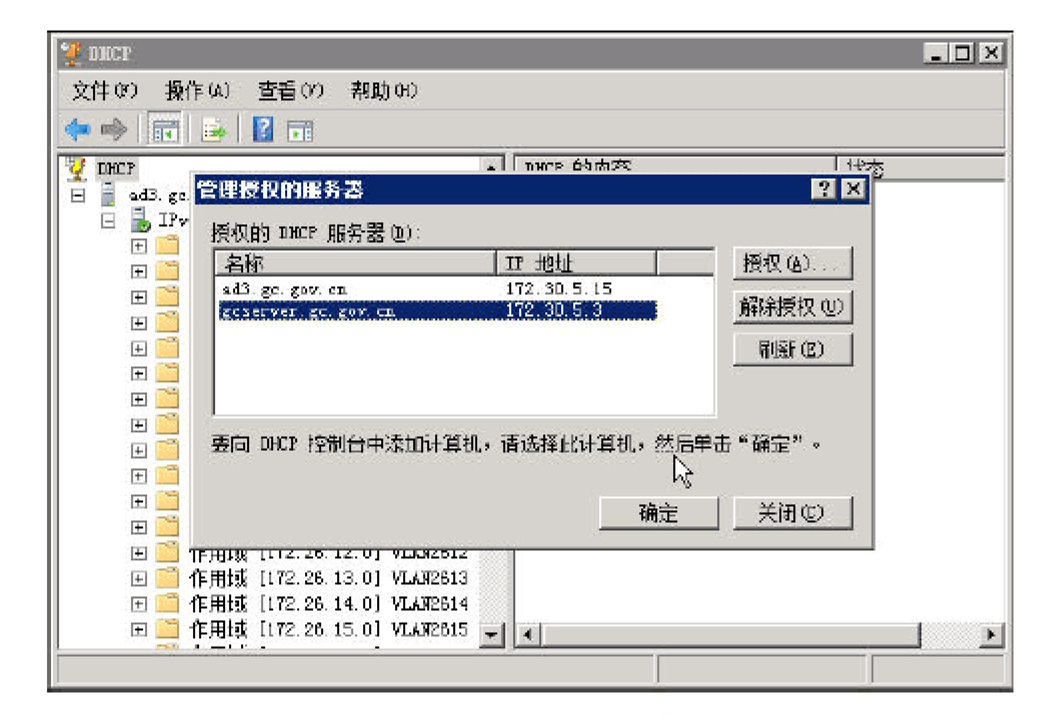


图 3-34　添加 DHCP 服务器的地址

04 在具有“Active Directory”的网络中，如果 DHCP 服务器没有“授权”，是不能为网络中的工作站分配 IP 地址的。

3.4　DHCP 客户机的设置和使用

配置完 DHCP 服务器后，下面来介绍如何配置 DHCP 客户端。

3.4.1　为 Windows XP 计算机启用 DHCP 客户端

在 Windows XP、Windows Server 2003 中，将计算机设置为 DHCP 客户端的方式及操作与 Windows 2000 系统相同，这里不再介绍。但从 Windows XP 系统开始，其客户端支持“备用配置”。在设置“备用配置”参数后，当 DHCP 客户端计算机不能从 DHCP 服务器获得地址时，将会使用“备用配置”的参数，具体设置步骤如下。

01 以管理员账户进入计算机，打开“网络连接”，双击“本地连接”，在打开的“本地连接属性”对话框中，双击“Internet 协议（TCP/IP）”，在打开的“Internet 协议（TCP/IP）属性”对话框中选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”，如图 3-35 所示。

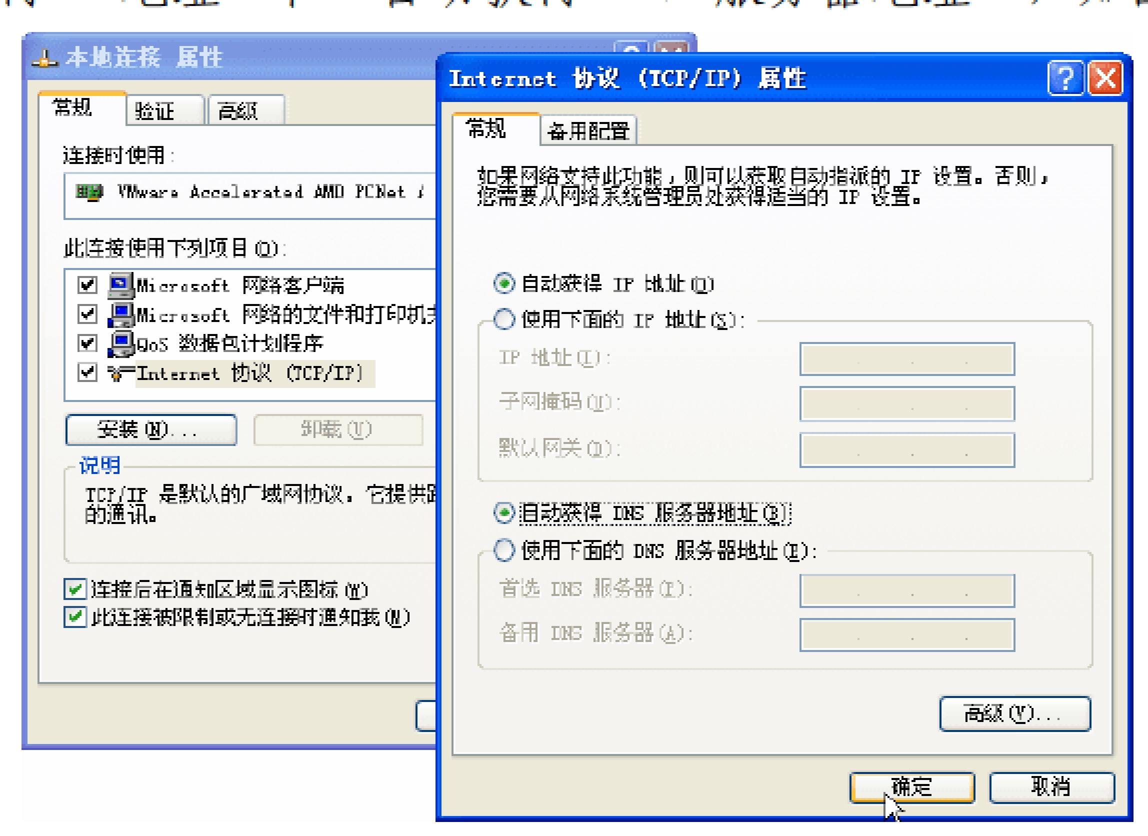


图 3-35　自动获得 IP 地址

02 Windows XP 的计算机，可以通过打开“本地连接”对话框，从“支持”选项卡中，查看 IP 地址等参数，如图 3-36 所示。还可以通过单击“详细信息”按钮，查看更多的参数，如 DNS、WINS 服务器地址等，如图 3-37 所示。

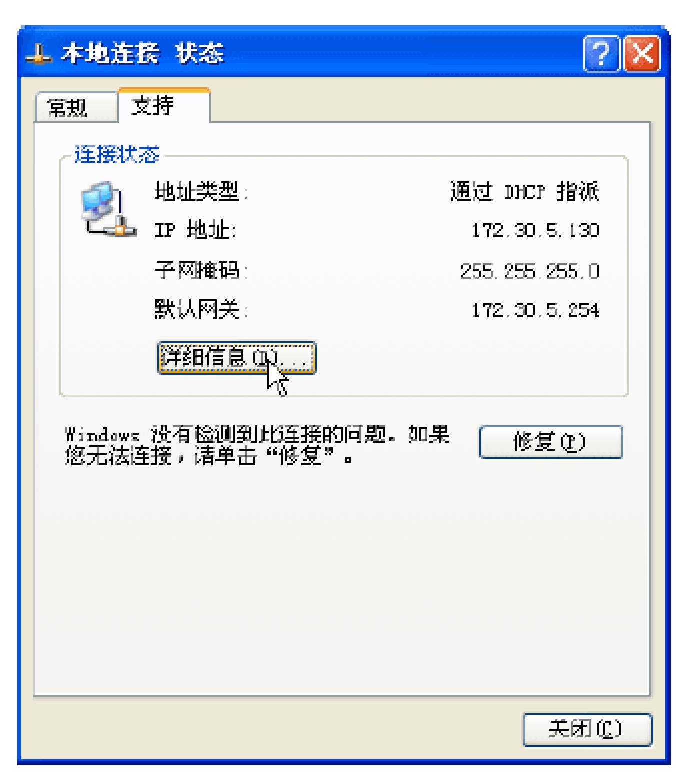


图 3-36　查看 IP 地址等参数

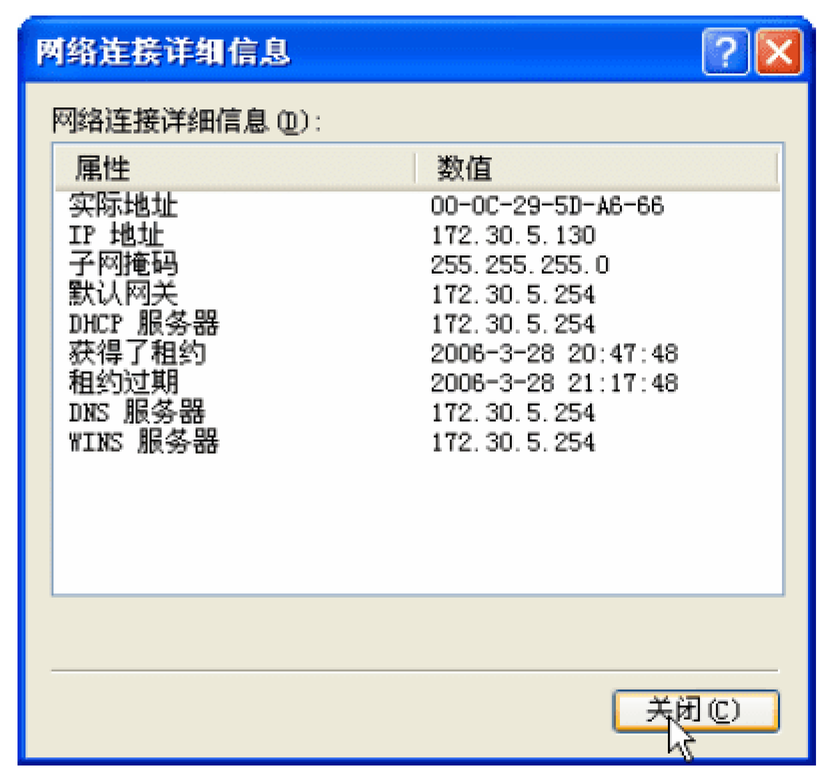


图 3-37　网络连接详细信息

而在 Windows XP 中，通过 ipconfig 命令查看、释放和重新获得地址，和在 Windows 2000 中相同，在此不再赘述。

3.4.2　为 Windows 7/2008 启用 DHCP 客户端

在 Windows 7、Windows Server 2008 中，启用 DHCP 客户端的步骤很简单，只要在“网络和共享中心”，进入 IP 地址设置对话框，选择“自动获得 IP 地址”和“自动获得 DNS 地址”即可，如图 3-38 所示。



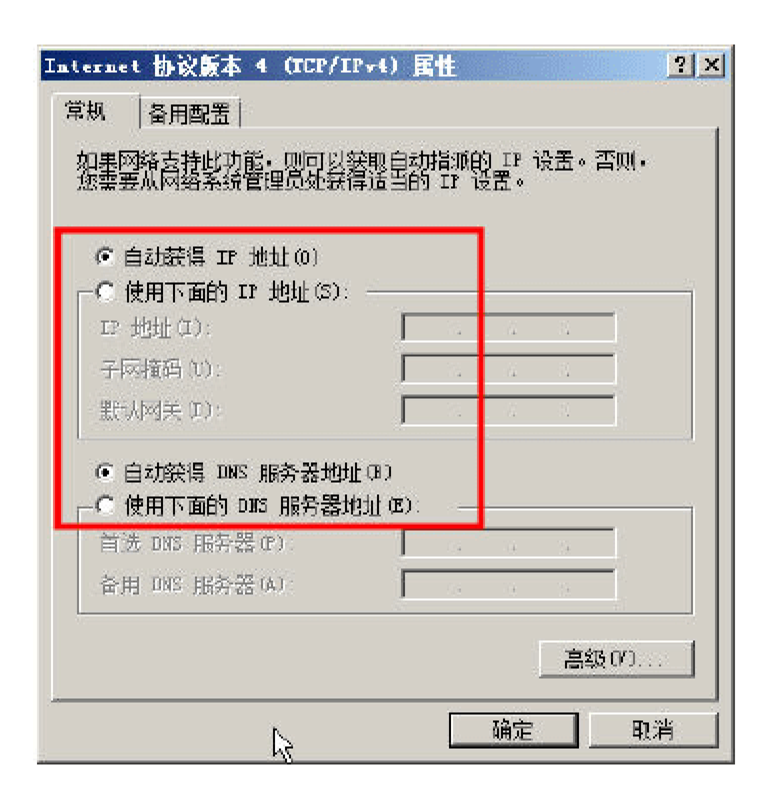


图 3-38　启用 DHCP 客户端

3.4.3　ipconfig 命令

对于管理员或高级用户来说，也可以使用 ipconfig 命令，查看当前的 IP 地址配置、重新从 DHCP 服务器获取 IP 地址等。ipconfig 的常用命令及参数如图 3-39 所示（进入命令提示符窗口，执行 ipconfig /all 得到）。

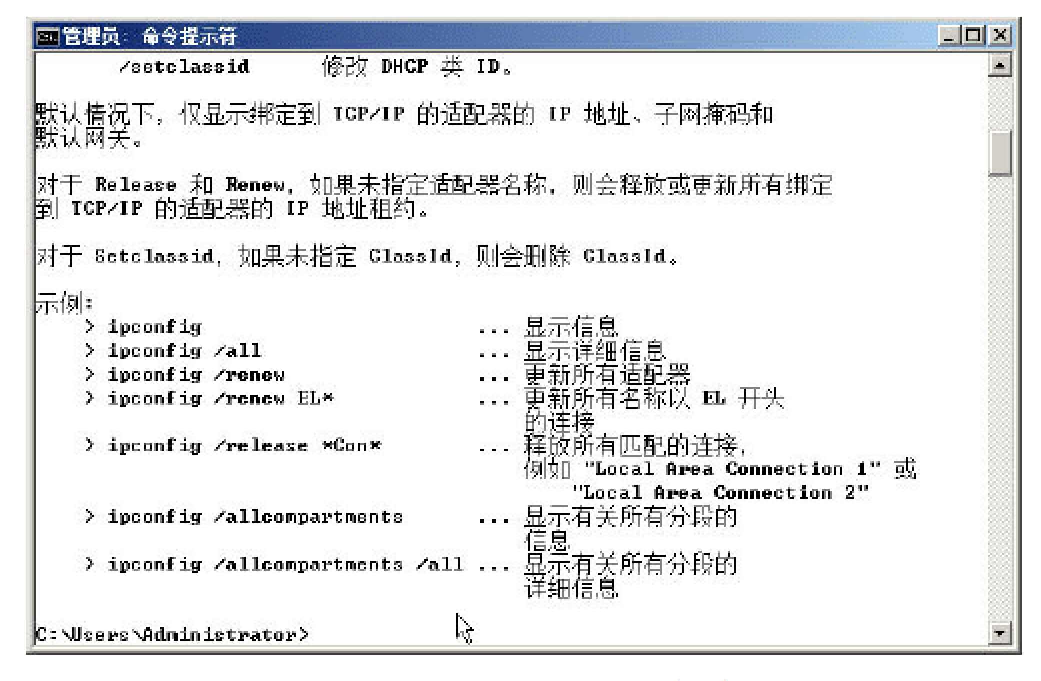


图 3-39　ipconfig 命令

常用的 ipconfig 命令参数有：

```
ipconfig /all:显示当前计算机所有网卡的所有网络参数
ipconfig /renew：更新网卡的参数，重新获得新的 IP 地址及参数
ipconfig /release：释放所有网卡的连接
ipconfig /flushdns：当空当前 DNS 的缓存信息
```

3.5　DNS 概述

在网络的初期，计算机之间主要用 IP 地址进行通信。但随着网络的扩大，IP 地址不容易记忆，这时引入了 DNS 概念。DNS 是典型的“客户/服务器”网络，包括 DNS 客户端和服务器端。DNS 客户端需要用 DNS 名称进行通信时，通过查找 DNS 服务器，用来获得 DNS 名称对应的 IP 地址，并将获得的 IP 地址用来通信。

DNS 服务器可以将 DNS 名称解析成 IP 地址，也可以将 IP 地址反向解析成 DNS 名称。本节介绍 Windows Server 2008 中 DNS 服务器的基础知识，以及 DNS 的安装配置。

3.5.1　DNS 服务器的基础知识

DNS 是域名系统（Domain Name System）的英文缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于局域网、广域网以及 Internet 等 TCP/IP 网络中，通过容易记忆的用户友好名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务器可以将此名称解析成和之相对应的其他信息，如 IP 地址。它也可以将 IP 地址反向解析成 DNS 名称。

例如，多数用户喜欢使用友好的名称（如 www.wangchunhai.cn）来查找计算机，如网络上的邮件服务器或 Web 服务器。友好名称更容易了解和记住。但是，计算机使用数字地址（目前为 IPv4 的地址，采用类似 123.22.33.44 的格式）在网络上进行通信。为了更容易地使用网络资源，DNS 等命名系统提供了一种方法，将计算机或服务的用户友好名称映射为数字地址。图 3-40 显示了 DNS 的基本用途，即根据易记的计算机名称查找其 IP 地址。

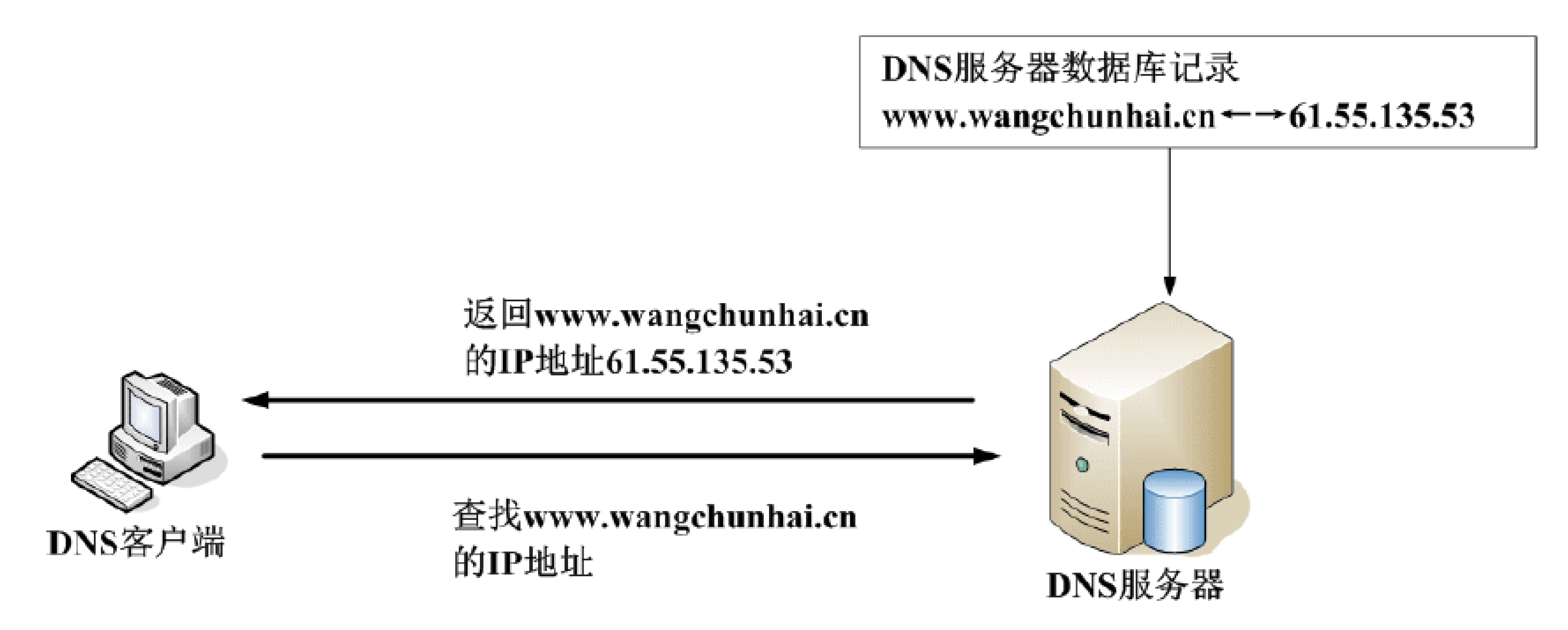


图 3-40　DNS 服务器的查询过程

在图 3-40 中，客户端计算机查询 DNS 服务器，要求获得某台计算机（已将其 DNS 域名配置为 wangchunhai.cn）的 IP 地址。由于 DNS 服务器能够根据其本地数据库应答此查询，因此，它将以包含所请求信息的应答来回复客户端，即一条主机（A）资源记录，其中含有 www.wangchunhai.cn 的 IP 地址信息。

3.5.2　DNS 系统结构

DNS 系统包括“DNS 域命名空间”、“DNS 资源记录”、“DNS 服务器”、“DNS 客户端”等四部分，其主要意义如下：

（1）DNS 域命名空间，它指定用于组织名称的域的层次结构。

（2）DNS 资源记录，它将 DNS 域名映射到特定类型的资源信息，以供在命名空间中注册或解析名称时使用。

（3）DNS 服务器，用于存储和应答资源记录的名称查询。

（4）DNS 客户端，也称作解析程序，用于查询服务器，以搜索并将名称解析为查询中指定的资源记录类型。

1. 了解 DNS 域命名空间

如图 3-41 所示，DNS 域命名空间基于命名域树的概念。树的每个等级都可代表树的一个分支或叶。分支是多个名称被用于标识一组命名资源的等级。叶代表在该等级中仅使用一次来指明特定资源的单个名称。

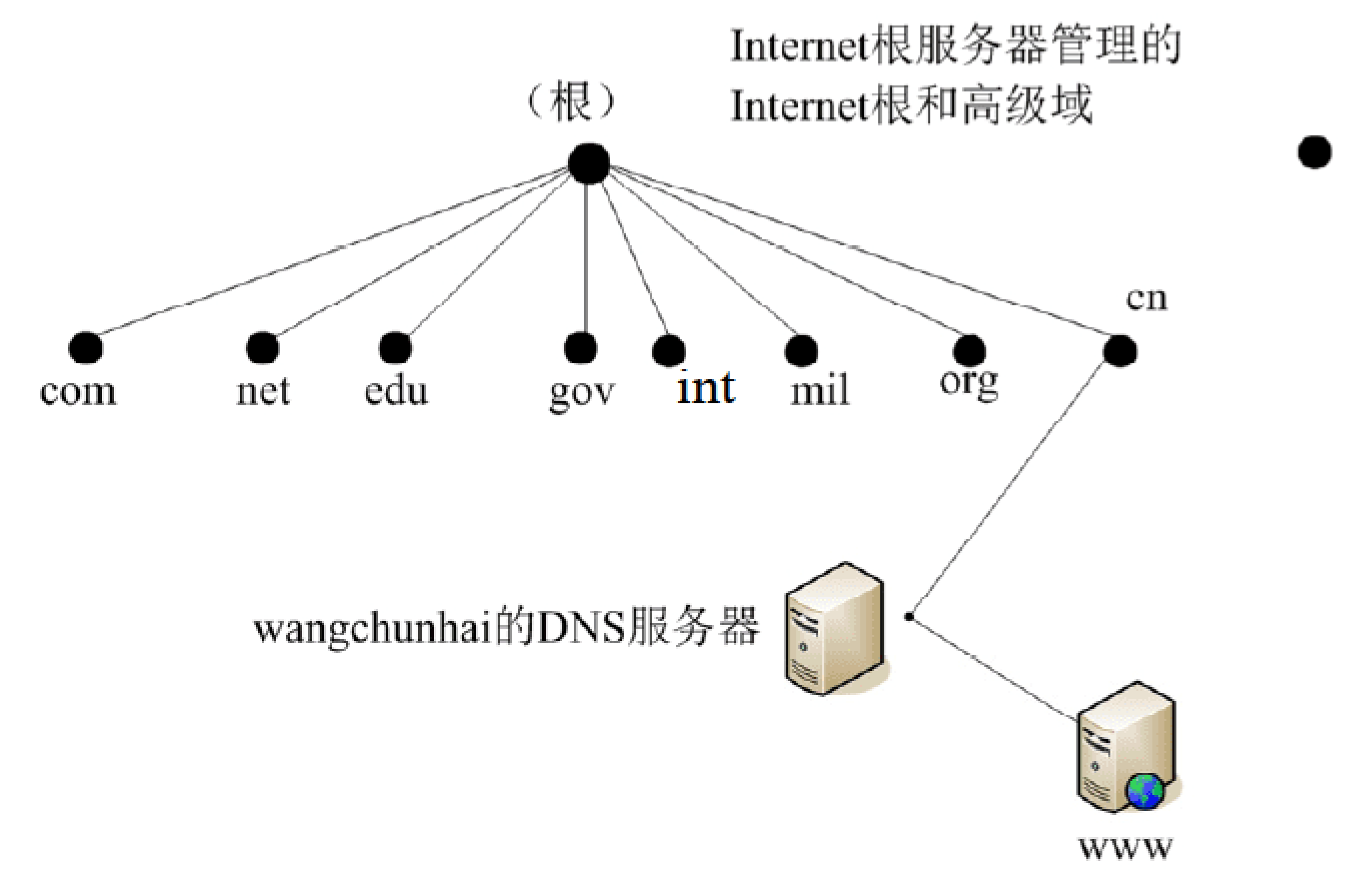


图 3-41　DNS 域命名空间

在图 3-41 中，DNS 域命名空间的最顶端是“根”服务器，用一个英文的句点表示，下面是顶级域和国家域，用来代表不同的机构和国家（例如，.com 表示商业性的公司）。在顶级域名下面可以注册域名，如本书作者个人的域名“wangchunhai.cn”就是在“.cn”下注册的域名，而“www.wangchunhai.cn”是在“wangchunhai.cn”的域名中注册的 A 记录。如果在“wangchunhai.cn”下注册域名，则表示“wangchunhai.cn”下的“二级域名”。在“二级域名”下还可以注册其他记录。

2. 如何组织 DNS 域命名空间

在树中使用的任何 DNS 域名从技术上说都是域。但是，大多数对 DNS 的讨论都是以 5 种方式之一标识名称，它以名称常用的等级和方式为基础。例如，注册到 wangchunhai（wangchunhai.cn）的 DNS 域名称作二级域。这是因为该名称有两个部分（称作标号），这两个部分显示它比树的顶级或根低两个等级。大多数 DNS 域名有两个或多个标号，每一个都表示树中的新等级。名称中使用句点分隔标号。

除二级域之外，表 3-2 介绍了根据其在命名空间中的功能来描述 DNS 域名所用的其他术语。

表 3-2　DNS 术语

名称类型	描述	示例
域根	这是树的顶级，它表示未命名的等级。 它有时显示为两个空引号（""），以表示空值。在 DNS 域名中使用时，它由尾部句点（.）表示，以指定该名称位于域层次结构的最高层或根。在这种情况下，DNS 域名被认为是完整名称并指向名称树中的确切位置。以这种方式表示的名称称作完全限定的域名（FQDN）	在名称末尾使用的单个句点（.），如“www.wangchunhai.cn.”
顶级域	由两三个字母组成的名称用于指示国家/地区或使用名称的单位类型。详细信息参阅表 3-3	“.com”，它表示在 Internet 上从事商业活动的公司注册的名称
二级域	为了在 Internet 上使用而注册到个人或单位的长度可变名称。这些名称始终基于相应的顶级域，这取决于单位的类型或使用的名称所在的地理位置	“zhangs.wangchunhai.cn.”，它是由 Internet DNS 域名注册人员注册到 wangchunhai 的二级域名
子域	单位可创建的其他名称，这些名称从已注册的二级域名中派生。包括为扩大单位中名称的 DNS 树而添加的名称，并将其分为部门或地理位置	“zhangs.wangchunhai.cn.”是由 wangchunhai 指派的虚拟子域，用于文档示例名称中
主机或资源名称	代表名称的 DNS 树中的叶节点并且标识特定资源的名称。DNS 域名最左边的标号一般标识网络上的特定计算机。例如，如果位于该层的名称在主机（A）资源记录（RR）中使用，则可以根据其主机名搜索计算机的 IP 地址	“www.zhangs.wangchunhai.cn.”，其中第一个标号（“www”）是网络上特定计算机的 DNS 主机名

表 3-3 是在 Internet 常用的顶级域列表，组织注册二级域名时通过类型对这些组织进行分类。例如，microsoft.com（注册到 Microsoft 的二级域名）在“com”域注册，因为这是为在 Internet 上从事商业活动的单位提供的顶级域。

表 3-3　Internet 常用的顶级域列表

顶级名称	描述	用于
arpa	属于美国国防部高级研究计划局（ARPA）。为 Internet 上使用 Internet 分配编号机构（IANA）分配给 DNS 域名的、Internet 协议版本 4（IPv4）地址的计算机，注册这些地址的反向映射	in-addr.arpa 域
com	供商业组织使用	商号和公司
edu	供教育机构使用	公立和私立学校、学院和大学
gov	供政府机构使用	地方、州和联邦政府机构
int	保留供国际组织使用。目前计划在 RFC 1886 中使用，为在 Internet 上使用 IANA 分配给在 ip6.int 域中 DNS 域名的 Internet 协议版本 6（IPv6）地址的计算机注册这些反向映射	ip6.int 域
mil	供军事机构使用	美国国防部（DoD）、美国海军、美国陆军、美国空军及其他军事机构
net	供提供大规模 Internet 或电话服务的组织使用	InterNIC、AT&T、其他大规模 Internet 和电话服务提供商
org	供非商业、非盈利单位使用	教堂和慈善机构
cn	代表中国	

3. 解释 DNS 域名

DNS 有一种标注和解释 DNS 域名完全合格路径的方法，类似于在命令提示符下标注或显示文件、目录完整路径的方法。

例如，目录树路径有助于指向文件存储在计算机上的确切位置。对于 Windows 计算机，反斜杠（\）指示通向确切的文件位置的每个新目录。对于 DNS，相当于名称中使用的每个新域等级的句点（.）。

例如，对于名为 Services 的文件，在 Windows 命令提示符下显示的该文件的完整路径应为：C:\Windows\System32\Drivers\Etc\Services。

要解释文件的完整路径，需要按照从左到右的顺序读名称，从最高或最概括的信息段（存储文件的驱动器 C）到最具体的信息，文件名“Services”。下面的例子显示了层次结构中指向驱动器 C 上 Services 文件位置的 5 个独立等级：

（1）驱动器 C 的根目录文件夹（C:\）。

（2）安装 Windows 的系统根目录文件夹（Windows）。

（3）存储系统组件的系统文件夹（System32）。

（4）存储系统设备驱动程序的子文件夹（Drivers）。

（5）存储系统和网络设备驱动程序所用的各种文件的子文件夹（Etc）。

对于 DNS，带有多级域名的示例如下，即完全限定的域名（FQDN）：host-a.example.microsoft.com。

和文件名示例不同的是，当从左到右读取时，DNS FQDN 从其最具体信息（名为“host-a”的计算机的 DNS 名称）移至其最高或最概括的信息段（尾部句点（.）指示 DNS 名称树的根）。该例显示了从“host-a”特定主机位置开始的 4 个独立 DNS 域等级：

（1）“example”域，对应于计算机名“host-a”注册使用的子域。

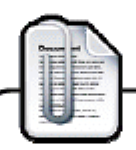
（2）“microsoft”域，对应于确定“example”子域的父域。

（3）“com”域，对应于由确定“microsoft”域的公司或商业单位指派使用的顶级域。

（4）尾部句点（.）是一个标准的分隔符字符，可用于使完整 DNS 域名限定到 DNS 命名空间树的根级。

4. 有关 DNS 和 Internet 的背景

由于需要为 Internet 上的计算机提供名称到地址的映射服务，因此开发了域名系统（DNS）。在 1987 年引入 DNS 之前，将容易记忆的计算机名称映射到 IP 地址的作法，主要通过使用称作主机文件的共享静态文件来进行。



说 明

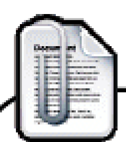
这个文件在 Windows 计算机中，保存在 hosts 文本文件中，通常在 c:\windows\system32\drivers\etc\hosts。

最初 Internet 非常小，仅使用一个集中管理的文件就可以通过 FTP 为连入 Internet 的站点发布和下载内容。每个 Internet 站点将定期地更新其主机文件的副本并且发布主机文件的更新版本来反映网络的变化。

当 Internet 上的计算机数增加时，通过一个中心授权机构，为所有 Internet 主机管理一个主机文件的工作将无法进行。文件会随着时间的推移而增大，这样按当前更新的形式维持文件以及将文

件分配至所有站点将更加困难。

制定 DNS 标准为主机文件提供可供选择的方案。RFC1034 和 1035 指定大多数核心协议，并且 RFC1034 和 1035 已添加至提交给 Internet 工程任务组（IETF）的其他 RFC 中，并由其他 RFC 更新。IETF 将继续审阅和通过新的草案，所以 DNS 的标准会根据用户需要不断发展和变化。



说 明

（1）DNS 域名在每个级别都要求是惟一的，但是单独的名称标号可在其他域中重新使用。例如，名称“mailserver”只能在 example.microsoft.com 和 microsoft.com 域中使用一次。

（2）支持将主机文件作为把主机 DNS 域名映射到其 IP 地址的本地静态文件。启动 DNS 客户端服务时，它会将添加到该文件的所有映射的项目预载到本地 DNS 名称缓存中。

（3）在%systemroot%\system32\drivers\etc\hosts 文件夹中提供了主机文件。要查看或修改该文件，可使用记事本程序或其他文本编辑器。

3.5.3 DNS 查询的工作过程和原理

当 DNS 客户端需要查询程序中使用的名称时，它会查询 DNS 服务器来解析该名称。客户端发送的每条查询消息都包括三条信息，指定服务器回答的问题：

- 指定的 DNS 域名，规定为完全合格的域名（FQDN）。
- 指定的查询类型，可根据类型指定资源记录，或者指定查询操作的专用类型。
- DNS 域名的指定类别。

对于 Windows DNS 服务器，它始终应指定为 Internet（IN）类别。例如，指定的名称可为计算机的 FQDN，如 host-a.example.microsoft.com，并且指定的查询类型用于通过该名称搜索地址 A 资源记录。将 DNS 查询看作客户端向服务器询问，由两部分组成的问题，如“您是否拥有名为‘hostname.example.microsoft.com’的计算机的 A 资源记录？”当客户端收到来自服务器的应答时，它将读取并解释应答的 A 资源记录，获取根据名称询问的计算机的 IP 地址。

DNS 查询以各种不同的方式进行解析。有时，客户端也可使用先前查询获得的缓存信息在本地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询。DNS 服务器也可代表请求客户端查询或联系其他 DNS 服务器，以便完全解析该名称，并随后将应答返回至客户端。这个过程称为递归。

另外，客户端自己也可尝试联系其他 DNS 服务器来解析名称。当客户端执行此操作时，它会根据来自服务器的参考答案，使用其他独立查询。这个过程称为迭代。

总之，DNS 查询进程分两部分进行：

- 名称查询从客户端计算机开始，并传输至解析程序，即 DNS 客户端服务程序进行解析。
- 不能在本地解析查询时，可根据需要查询 DNS 服务器来解析名称。

下面将详细地解释这两个过程。

1. 本地解析程序

图 3-42 显示了完整的 DNS 查询进程。

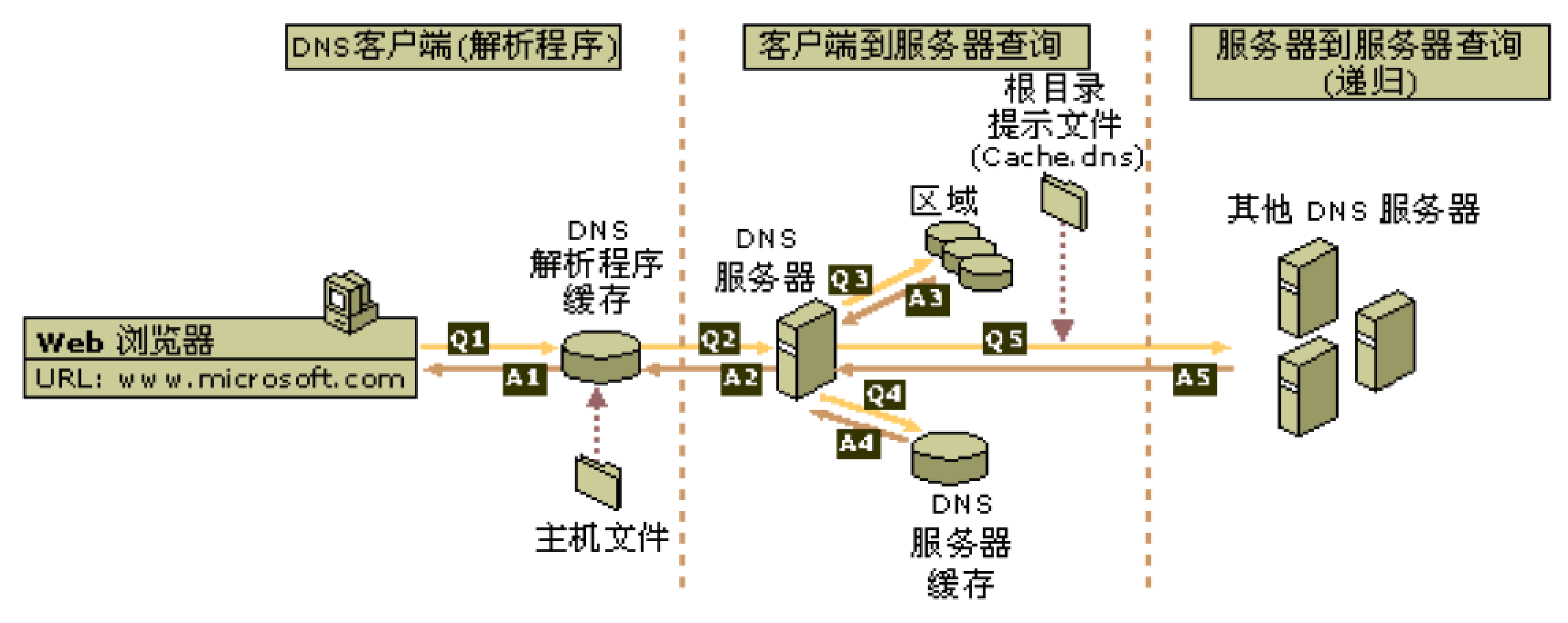


图 3-42　DNS 查询进程

在图 3-42 中，DNS 域名由本机的程序使用。该请求随后传输至 DNS 客户端服务，以便使用本地缓存信息进行解析。如果可以解析查询的名称，则应答该查询，该进程完成。

本地解析程序的缓存可包括从两个可能的来源获取的名称信息：

- 如果在本地配置主机文件，则来自该文件的任何主机名称到地址的映射，在 DNS 客户端服务启动时将预先加载到缓存中。
- 从以前的 DNS 查询应答的响应中获取的资源记录，将被添加至缓存并保留一段时间。

如果此查询和缓存中的项目不匹配，则解析过程继续进行，客户端查询 DNS 服务器来解析名称。

2. 查询 DNS 服务器

当 DNS 服务器接收到查询时，首先检查它能否根据在服务器的本地配置区域中获取的资源记录信息作出权威性的应答。如果查询的名称和本地区域信息中的相应资源记录匹配，则使用该信息来解析查询的名称，服务器作出权威性的应答。

如果区域信息中没有查询的名称，则服务器检查它能否通过先前查询的本地缓存信息来解析该名称。如果从中发现匹配的信息，则服务器使用该信息应答查询。接着，如果首选服务器可使用来自其缓存的完全匹配响应来应答发出请求的客户端，则此次查询完成。

如果查询名称在首选服务器中未发现来自缓存或区域信息的匹配应答，则查询进程可继续进行，使用递归来完全解析名称。这涉及来自其他 DNS 服务器的支持，以帮助解析名称。在默认情况下，DNS 客户端服务要求服务器在返回应答之前，使用递归过程来代表客户端完全解析名称。在大多数情况下，DNS 服务器默认配置为支持递归过程，如图 3-43 所示。

为了使 DNS 服务器正确执行递归过程，首先需要使用 DNS 域命名空间内有关其他 DNS 服务器的一些有用的联系信息。该信息以根提示的形式提供，它是一个初始资源记录列表，DNS 服务可利用这些记录定位其他 DNS 服务器，它们对 DNS 域命名空间树的根具有绝对控制权。根服务器对于 DNS 域命名空间树中的根域和顶级域具有绝对控制权。

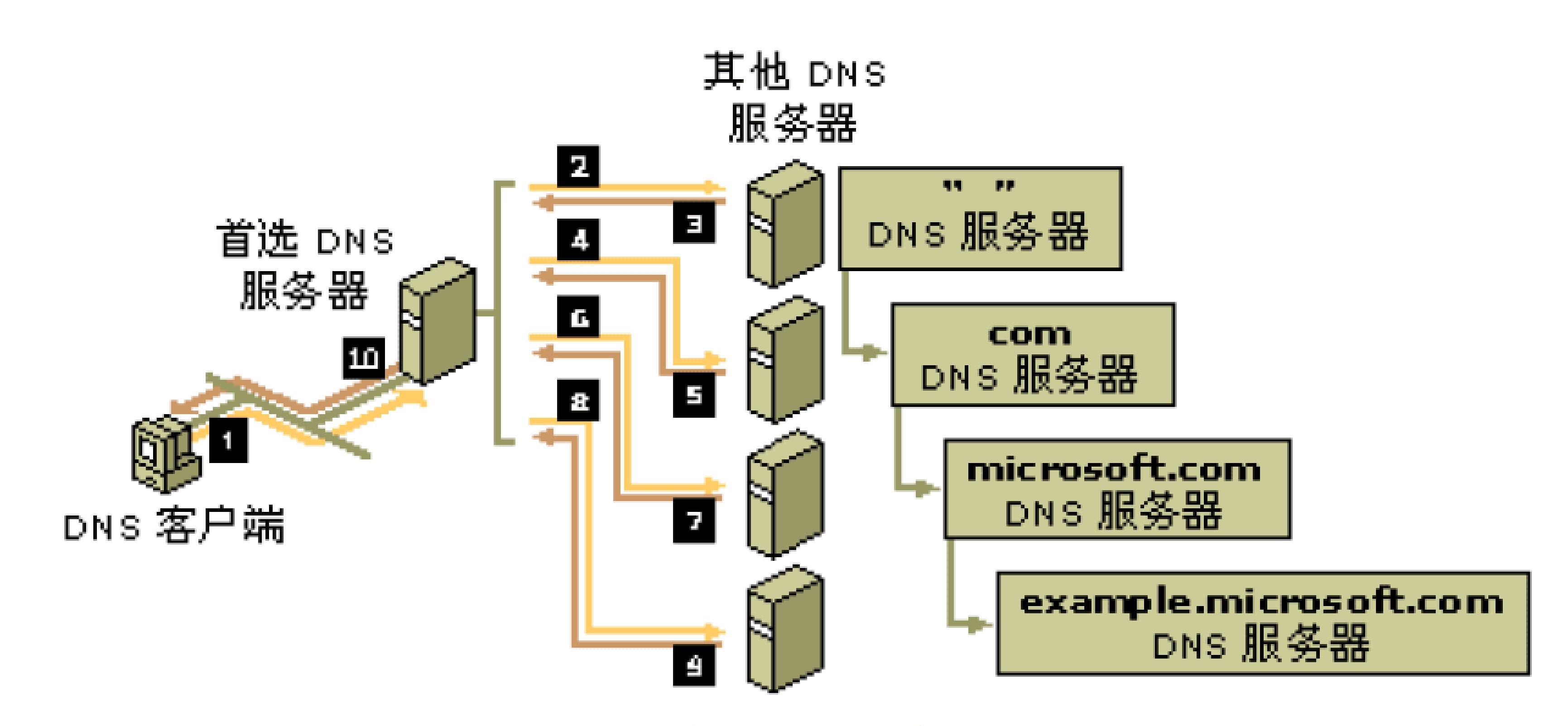


图 3-43 查询 DNS 服务器过程

使用根提示查找根服务器，DNS 服务器可完成递归的使用。理论上，该进程将启用 DNS 服务器，以定位那些对域命名空间树的任何级别使用的任何其他 DNS 域名具有绝对控制权的服务器。

例如，当客户端查询单个 DNS 服务器时，考虑使用递归过程来定位名称 host-b.example.microsoft.com。在 DNS 服务器和客户端首次启动，并且没有本地缓存信息可帮助解析名称查询时，就会进行上述过程。根据其配置的区域，它假定由客户端查询的名称是域名，该服务器在本地不包含有关该域名的信息。

首先，选择服务器分析全名并确定对于顶级域“com”具有绝对控制权的服务器的位置。其次，对“com”DNS 服务器使用迭代查询，以获取“microsoft.com”服务器的参考信息。然后，参考应答从“microsoft.com”服务器传送到“example.microsoft.com”的 DNS 服务器。最后，与服务器 example.microsoft.com 建立联系。因为该服务器包括作为其配置区域一部分的查询名称，所以它向启动递归的源服务器作出权威性的应答。当源服务器接收到表明已获得对请求查询的权威性应答的响应时，它将此应答转发给发出请求的客户端，这样递归查询过程就完成了。

尽管执行上述递归查询过程可能需要占用大量资源，但对于 DNS 服务器来说它仍然具有一些性能上的优势。例如，在递归过程中，执行递归查询的 DNS 服务器可获得有关 DNS 域命名空间的信息。该信息由服务器缓存起来并可再次使用，以便提高使用此信息或和之匹配的后续查询的应答速度。随着时间的推移，这些缓存信息会不断增加并占据大量的服务器内存资源，不过每次 DNS 服务重新启动时这一信息将被清除。

3. 可选的查询响应

以前对 DNS 查询的讨论，都假定此过程在结束时会向客户端返回一个肯定的响应。然而，查询也可返回其他应答。最常见的应答有：

- 权威性应答：权威性应答是返回至客户端的肯定应答，并随 DNS 消息中设置的“授权机构”位一同发送，消息指出此应答是从带直接授权机构的服务器获取的。
- 肯定应答：肯定应答可由查询的 RR 或 RR 列表（也称作 RRset）组成，它和查询的 DNS 域名和查询消息中指定的记录类型相符。
- 参考性应答：参考性应答包括查询中名称或类型未指定的其他资源记录。如果不支持递归过程，则这类应答将返回至客户端。这些记录的作用是为了提供一些有用的参考性应答，

客户端可使用参考性应答继续进行递归查询。参考性应答包含其他数据，如不属于查询类型的资源记录（RR）。例如，如果查询主机名称为“www”并且在这个区域未找到该名称的 ARR，而是找到了“www”的 CNAMERR，则 DNS 服务器在响应客户端时可包含该信息。

如果客户端能够使用迭代过程，则它可使用这些参考性信息为自己进行其他查询，以便完全解析此名称。

- 否定应答：来自服务器的否定应答可以表明，当服务器试图处理并且权威性地彻底解析查询的时候，遇到的两种可能的结果：
  - 权威性服务器报告：在 DNS 命名空间中没有查询的名称。
  - 权威性服务器报告：查询的名称存在，但该名称不存在指定类型的记录。

以肯定或否定响应的形式，解析程序将查询结果传回请求程序并把响应消息缓存起来。

- 如果查询的最终应答太长而不能在一个 UDP 消息数据包中发送和解析，则 DNS 服务器可以在 TCP 端口 53 上发送故障转移响应消息，以便在 TCP 连接会话中完全应答客户端。
- 当限定 DNS 客户端的名称解析到特定的 DNS 服务器（如 Intranet 上的 DNS 服务器）的时候，系统通常会禁止在 DNS 服务器上使用递归。当 DNS 服务器不能解析外部 DNS 名称的时候，可能也会禁用递归，而且期望客户端故障转移到其他 DNS 服务器，以便解析这些名称。在相应服务器的 DNS 控制台中，可以在“高级”属性中进行配置，以禁用递归。
- 如果在 DNS 服务器上禁用递归，那么将无法在同一服务器上使用转发器。
- 默认情况下，在执行递归查询并联系其他 DNS 服务器时，DNS 服务器使用若干默认的时间设置。它们是：
  - 3 秒的递归重试间隔：这是 DNS 服务在递归查询期间重试查询之前等候的时间长度。
  - 15 秒的递归超时间隔：这是 DNS 服务在重试的递归查询失败之前等候的时间长度。

在大多数情况下，这些参数不需要进行调整。但是，如果在慢速广域网链路上使用递归查询，那么或许可通过对设置略作调整，来改善服务器的性能，加快查询的完成速度。

4. 迭代的工作原理

迭代是在以下条件生效时，DNS 客户端和服务器之间使用的名称解析类型：

- 客户端申请使用递归过程，但在 DNS 服务器上禁用递归。
- 查询 DNS 服务器时客户端没有申请使用递归。

来自客户端的迭代请求告知DNS服务器：客户端希望直接从DNS服务器那里得到最好的应答，无须联系其他 DNS 服务器。

使用迭代时，DNS 服务器根据它自身对和查询的名称数据有关的命名空间的特定知识应答客户端。例如，如果 Internet 上的 DNS 服务器接收到来自本地客户端“www.microsoft.com”的查询，则可能会返回来自其名称缓存的应答。如果查询的名称当前未存储在服务器的名称缓存中，则服务器可能会通过提供参考信息对客户端作出响应，即提供一张和客户端所查询的名称比较接近的其他

DNS 服务器的 NS 和 A 资源记录列表。

在形成参考信息的时候，假定 DNS 客户端负责向其他配置的 DNS 服务器继续进行递归查询，以便解析该名称。例如，在大多数情况下，DNS 客户端可能会将其搜索扩展到 Internet 上的根域服务器，以定位对于"com"域具有绝对控制权的 DNS 服务器。一旦联系上 Internet 根服务器，它就会从指向"microsoft.com"域的实际 Internet DNS 服务器中获得进一步的递归响应。当客户端收到这些 DNS 服务器的记录时，可以向 Internet 上的外部 Microsoft DNS 服务器发送其他迭代查询，它们可以提供肯定和权威性的应答。

使用迭代时，除了向客户端提供最好的应答外，DNS 服务器还可在名称查询解析中提供进一步的帮助。对于大部分迭代查询，如果它的主 DNS 不能辨识该查询，那么客户端使用本地配置的 DNS 服务器列表，在整个 DNS 命名空间中联系其他名称服务器。

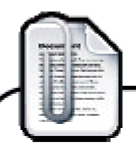
5. 缓存的工作原理

DNS 服务器采用递归或迭代来处理客户端查询时，它们将发现并获得大量有关 DNS 命名空间的重要信息，这些信息由服务器缓存。

缓存为 DNS 解析名称的后续查询提供了加速性能的方法，同时大大减少了网络上和 DNS 相关的查询通信量。

当 DNS 服务器代表客户端进行递归查询时，它们将暂时缓存资源记录（RR）。缓存的 RR 包含从 DNS 服务器获得的信息，对于进行迭代查询以便搜索和充分应答代表客户端所执行的递归查询过程中所获知的 DNS 域名而言，此信息具有绝对的权威性。稍后，当其他客户端发出新的查询，请求和缓存的 RR 匹配的 RR 信息时，DNS 服务器可以使用缓存的 RR 信息来应答它们。

当信息缓存时，生存时间（TTL）值适用于所有缓存的 RR。只要缓存 RR 的 TTL 没有到期，DNS 服务器就可继续缓存并再次使用 RR 来应答和这些 RR 相匹配的客户端提出的查询。将大部分区域配置中 RR 所用的缓存 TTL 值指定为"最小的（默认）TTL"，它被设置为用于区域的起始授权机构（SOA）资源记录。在默认情况下，最小的 TTL 为 3600 秒（1 小时），但可以进行调整，也就是说如果需要可以在每个 RR 上分别设置各自的缓存 TTL。



说 明

（1）可将 DNS 服务器安装为仅用于缓存服务器。

（2）默认情况下，DNS 服务器使用根提示文件 Cache.dns，该文件存储在服务器计算机的 %systemroot%\System32\Dns 文件夹中。当服务启动时，该文件的内容预先加载到服务器存储区，并包含运行 DNS 服务器所在的 DNS 命名空间的根服务器的指针信息。

3.5.4 DNS 的反向查找

在大部分的 DNS 查找中，客户端一般执行正向查找。正向查找是基于存储在地址（A）资源记录中的另一台计算机的 DNS 名称的搜索。这类查询希望将 IP 地址作为应答的资源数据。

DNS 也提供反向查找过程，允许客户端在名称查询期间使用已知的 IP 地址，并根据它的地址查找计算机名。反向查找采取问答形式，如"您能告诉我使用 IP 地址 192.168.1.20 的计算机的 DNS 名称吗？"

DNS 最初在设计上并不支持这类查询。支持反向查询过程可能存在一个问题，即 DNS 名称空间如何组织和索引名称，IP 地址如何分配，这些方面都有差别。如果回答以前问题的惟一方式是在 DNS 名称空间中的所有域中搜索，那么反向查询必需花很长时间，需要进行很多处理，才能真正有用。

为了解决该问题，在 DNS 标准中定义了特殊域 in-addr.arpa 域，并保留在 Internet DNS 名称空间中，以便提供切实可靠的方式执行反向查询。为了创建反向名称空间，in-addr.arpa 域中的子域是按照带点的十进制表示法编号的 IP 地址的相反顺序构造的。

因为和 DNS 名称不同，当从左向右读取 IP 地址时，它们是以相反的方式解释的，所以需要将域中的每个八位字节数值反序排列。从左向右读 IP 地址时，读取顺序是从地址的第一部分一般的信息（IP 网络地址）到最后八位字节中包含的更具体的信息（IP 主机地址）。

因此，创建 in-addr.arpa 域树的时候，IP 地址八位字节的顺序必需倒置。DNS in-addr.arpa 树的 IP 地址可以委派给某些公司，因为已为它们分配了 Internet 定义的地址类内特定的或有限的 IP 地址集。

最后，在 DNS 中建立的 in-addr.arpa 域树要求定义其他资源记录（RR）类型，如指针（PTR）RR。这种 RR 用于在反向查找区域中创建映射，它一般对应于其正向查找区域中，某一主机的 DNS 名的主机（A）命名的 RR。

3.5.5　DNS 转发器

转发器是网络上的域名系统（DNS）服务器，用来将外部 DNS 名称的 DNS 查询转发给该网络外的 DNS 服务器。也可使用“条件转发器”按照特定域名转发查询。

通过网络中的其他 DNS 服务器将它们在本地无法解析的查询转发给网络上的 DNS 服务器，该 DNS 服务器即被指定为转发器。使用转发器可管理网络外的名称解析（如 Internet 上的名称），并改进网络中计算机的名称解析效率。

图 3-44 显示了如何使用转发器定向外部名称查询。

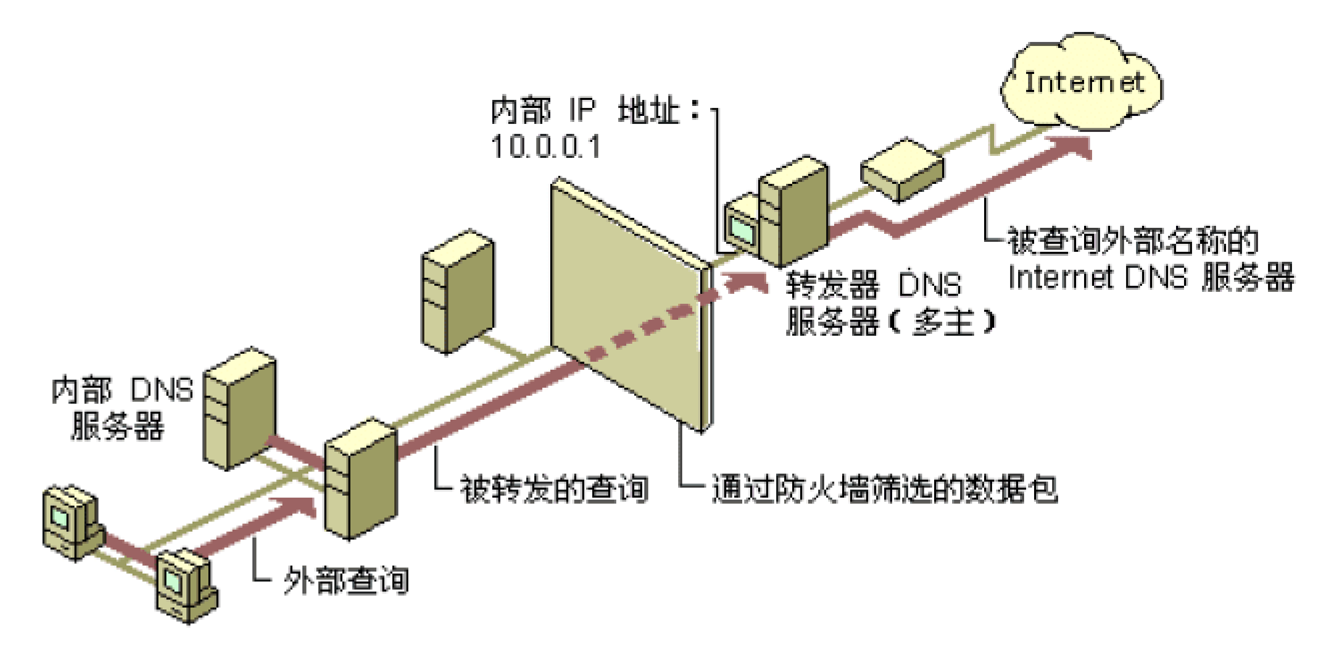


图 3-44　使用 DNS 转发器

如果没有将特定 DNS 服务器指定为转发器，则所有 DNS 服务器都能够使用其根提示向网络外发送查询。这样，许多内部可能非常重要的 DNS 信息都会暴露在 Internet 上。除了安全和隐私问题，该解析方法还会导致大量外部通信，这种通信费用昂贵，将导致 Internet 连接的网络速度很慢或 Internet 服务成本很高、公司效率低下。

将 DNS 服务器指定为转发器时，转发器将负责处理外部通信，从而将 DNS 服务器有限地暴露给 Internet。转发器将建立外部 DNS 信息的巨大缓存，因为网络中的所有外部 DNS 查询都是通过它解析的。在很短的时间内，转发器将使用该缓存数据解析大部分外部 DNS 查询，从而减少网络的 Internet 通信和 DNS 客户端的响应时间。

配置为使用转发器的 DNS 服务器和未配置为使用转发器的 DNS 服务器的行为不同。配置为使用转发器的 DNS 服务器的行为如下：

（1）当 DNS 服务器收到查询时，它会尝试主持和缓存主要和辅助区域解析该查询。

（2）如果不能使用该本地数据解析查询，它会将查询转发给指定为转发器的 DNS 服务器。

（3）在尝试和 DNS 服务器的根提示中指定的 DNS 服务器联系之前，该 DNS 服务器会等待一段很短的时间，等待来自转发器的应答。

当 DNS 服务器将查询转发给转发器时，它会为转发器发送递归查询。这和迭代查询不同，在标准名称解析（不涉及转发器的名称解析）期间，DNS 服务器将迭代查询发送给另一个 DNS 服务器。

3.5.6　动态更新

动态更新允许 DNS 客户端计算机在发生更改的任何时候使用 DNS 服务器注册和动态地更新其资源记录。它减少了对区域记录进行手动管理的次数，对于频繁移动或改变位置并使用 DHCP 获得 IP 地址的客户端更是如此。

DNS 客户端和服务器服务支持使用动态更新。DNS 服务器服务允许配置在加载标准主要区域或目录集成区域的每个服务器上，在每个区域上启用或禁用动态更新。默认情况下，DNS 客户端服务在配置用于 TCP/IP 时，将动态更新 DNS 中的主机（A）资源记录（RR）。

默认情况下，静态配置用于 TCP/IP 的计算机尝试为由其安装的网络连接所配置和使用的 IP 地址动态注册主机（A）和指针（PTR）资源记录（RR）。默认情况下，所有计算机都基于其完全限定的域名（FQDN）注册记录。

3.5.7　Active Directory 集成

Active Directory 是从 Windows 2000 Server 开始的一项服务，用于替代以前的 Windows NT Server 中的“域”。从 Windows 2000 Server 开始，DNS 服务器服务已集成到 Active Directory 的设计和实施中。Active Directory 提供了用于组织、管理和定位网络资源的企业级工具。

1. DNS 如何和 Active Directory 集成

在服务器上安装 Active Directory 时，可以将服务器升级为指定域的域控制器角色。完成该过程时，系统将提示为要加入和升级服务器的 Active Directory 域指定 DNS 域名。

如果在该过程中，指定域的权威 DNS 服务器在网络上找不到，或不支持 DNS 动态更新协议，系统将提示通过相关选项安装 DNS 服务器。之所以提供该选项，原因在于定位该服务器或作为 Active Directory 域成员的其他域控制器时需要 DNS 服务器。

安装 Active Directory 之后，对新的域控制器上运行的 DNS 服务器操作时，可以使用两种存储和复制区域的选项：

- 使用基于文本文件的标准区域存储。按这种方式存储的区域位于.Dns 文件中，这些文件存储在运行 DNS 服务器的每台计算机上的 systemroot\System32\Dns 文件夹中。区域文件名称和创建区域时为区域选择的名称相对应，如区域名称为 example.microsoft.com 时的 example.microsoft.com.dns。
- 使用 Active Directory 数据库的目录集成区域存储。按这种方式存储的区域位于域或应用程序目录分区下的 Active Directory 树中。每个目录集成区域都存储在按照创建该区域时为它选择的名称标识的 dns Zone 容器对象中。

2. Active Directory 集成的好处

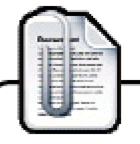
要对网络上的 DNS 进行配置以支持 Active Directory，强烈建议使用集成目录的主要区域，因为这样做可以提供以下好处：

（1）基于 Active Directory 功能的多主机更新和增强的安全性。在标准区域存储模式中，以单主机更新模式为基础进行 DNS 更新。在该模式中，区域的单个授权 DNS 服务器被指派为该区域的主要源服务器。该服务器在本地文件中保留了相关区域的主控副本。通过该模式，该区域的主服务器代表一个固定的故障点。如果该服务器不可用，将不会对该区域处理来自 DNS 客户端的更新请求。

通过和目录集成的存储区，可以根据多主机更新模式对 DNS 进行动态更新。在该模式下，任何授权 DNS 服务器（如运行 DNS 服务器的域控制器）都被指定为该区域的主要源服务器。因为区域的主控副本完全复制到所有域控制器的 Active Directory 数据库中，所以该区域可由任何域控制器上运行的 DNS 服务器更新。

通过 Active Directory 的多主机更新模式，只要域控制器在网络上可用而且可以访问，和目录集成的区域的任何主服务器都可以处理来自 DNS 客户端的更新区域请求。

另外，在使用和目录集成的区域时，可以使用访问控制列表（ACL）的编辑功能，以确保目录树中 dnsZone 对象容器的安全。使用该功能，可以对区域或区域中指定的 RR 进行粒度访问。例如，可以对区域 RR 的 ACL 进行限制，以便只允许对指定的客户机或安全组（如域管理员组）进行动态更新。该功能不适用于标准主要区域。



说 明

如果将区域类型改为集成目录类型，默认情况下，更新区域时只允许进行安全更新。此外，只有可以对和 DNS 有关的 Active Directory 对象使用 ACL 时，ACL 才能应用到 DNS 客户端服务。

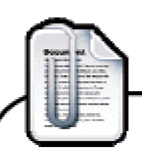
（2）只要将新的区域添加到 Active Directory 域，区域就会自动复制并同步至新的域控制器。尽管可以有选择地从域控制器中删除 DNS 服务，但和目录集成的区域已存储在每个域控制器中，因此，区域存储和管理不是附加的资源。另外，和可能需要传输整个区域的标准区域更新方法相比，同步存储目录信息的方法可以提高性能。

（3）通过将 DNS 区域数据库的存储集成到 Active Directory 中，可以针对网络简化数据库复制规划。分别存储和复制 DNS 名称空间和 Active Directory 域时，需要对其单独进行规划和管理。例如，将标准 DNS 区域存储和 Active Directory 结合使用时，需要设计、实现、测试和维护两个不

同的数据库复制拓扑结构。例如，在域控制器之间复制目录数据时需要使用一种复制拓朴结，而在 DNS 服务器之间复制区域数据库时需要使用另外一种复制拓扑结构。

在网络的规划和设计及其可能的最终扩展方面，这样做可能会产生额外的管理复杂性。通过集成 DNS 存储区，可以把与 DNS 和 Active Directory 有关的存储管理和复制问题统一起来，将它们合并为一个管理实体，并作为一个管理实体查看。

（4）和标准 DNS 复制相比，目录复制更快捷、更有效。因为 Active Directory 复制处理是基于每个属性进行的，所以只能传播相关的更改，这样可以减少更新目录存储区域时使用和提交的数据。



说 明

（1）该目录中只能存储主要区域。DNS 服务器不能在目录中存储辅助区域。因此，它必需在标准文本文件中存储这些数据。如果将所有的区域都存储在 Active Directory 中，Active Directory 的多主机复制模式将不再需要辅助区域。

（2）DNS 服务器服务包含这样一个选项，可以通过读取存储在 Active Directory 数据库和服务器注册表中的参数初始化 DNS 服务器服务。这是默认启动选项。

3.5.8 安装 Active Directory 的 DNS 要求

在成员服务器上安装 Active Directory 时，可将成员服务器升级为域控制器。Active Directory 将 DNS 作为域控制器的位置机制，使网络上的计算机可以获取域控制器的 IP 地址。

在 Active Directory 安装期间，在 DNS 中动态注册服务（SRV）和地址（A）资源记录，这些记录是域控制器定位程序（Locator）机制功能成功实现所必需的。

要在域或林中查找域控制器，客户端将在 DNS 中查询域控制器的 SRV 和 A 资源记录，这些资源记录为客户端提供域控制器的名称和 IP 地址。在这种环境中，SRV 和 A 资源记录被称为定位程序 DNS 资源记录。

向林中添加域控制器时，将使用定位程序 DNS 资源记录更新 DNS 服务器上主持的 DNS 区域，同时标识域控制器。为此，DNS 区域必需允许动态更新，同时，主持该区域的 DNS 服务器必需支持 SRV 资源记录才能公布 Active Directory 目录服务。如果主持权威 DNS 区域的 DNS 服务器不是运行 Windows 2000 或 Windows Server2003 的服务器，则应与 DNS 管理员联系，确定该 DNS 服务器是否支持所需的标准。如果服务器不支持所需标准，或者权威 DNS 区域不能被配置为允许动态更新，则需要对现有 DNS 结构进行修改。

3.6 DNS 服务器的安装与配置

在 Windows Server 2003、Windows Server 2008 中，只有“标准”的 DNS 服务器才需要配置，如果是 Active Directory 中的 DNS 服务器，通常系统会自动配置。而 Active Directory 中的 DNS 服务器，除了系统自动创建的一些记录外，其他设置和“标准”DNS 服务器都是一样的，所以本章

主要讲述“标准”DNS 服务器的安装配置。

作为实用的 DNS 服务器，有服务于 Internet 并为 Internet 上的其他用户提供 DNS 解析和查询的 DNS 服务器，也有专门用于内网并为内网的 DNS 解析提高解析速度的“DNS 缓存”服务器，许多时候，在内网架设 DNS 服务器可以用来解析由于“内、外网”DNS 解析不同所带来的网络通信问题。

接下来，介绍 DNS 服务器的安装和配置。本节将创建如下 DNS 服务器：

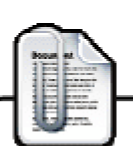
```
DNS 域名：msft.com
DNS 服务器地址：192.168.128.5
```

在 msft.com 域中创建 www、ftp 等记录，使其解析到 192.168.128.5。

3.6.1　安装 DNS 服务器

DNS 服务器的安装比较简单，基本上和安装 DHCP 服务器类似，主要步骤如下。

01 在将要安装 DNS 服务器的计算机中，检查 IP 地址，在本例中，设置 IP 地址为 192.168.128.5，DNS 地址为 192.168.128.5。



说 明

在实际的使用中，应该在 DNS 的客户端设置 DNS 的地址，为 DNS 服务器的 IP 地址。在本例中，设置 DNS 的地址为自己的，是为了实验的方便。

02 参照前文安装 DHCP 服务器的步骤，进入“服务器管理器→添加角色向导”对话框，在“选择服务器角色”选项组中，选中并添加“DNS 服务器”，如图 3-45 所示。

03 在“DNS 服务器”对话框，显示了 DNS 服务器的简介信息，查看之后单击“下一步”按钮，如图 3-46 所示。



图 3-45　添加 DNS 服务器

图 3-46　DNS 服务器简介

04 在“确认安装选择”对话框中，查看安装配置，单击“安装”按钮，开始安装。

05 DNS 服务器开始安装，安装完成之后，单击“关闭”按钮，完成安装。

3.6.2　创建正向查找区域

安装好 DNS 服务器之后，DNS 服务器只是一个“空”的数据库，需要在 DNS 服务器中创建“区域”之后，才能为对应的区域提供域名解析的服务（对于不能解析的域名，如果当前 DNS 服务器能连接到 Internet，将转发到 Internet 的“转发器”或“根”域名服务器进行转发）。在本例中，在新建的 DNS 服务器中创建名为 msft.com 的正向区域（为 msft.com 域提供域名解析服务），步骤如下。

01 在“服务器管理器”中定位到“角色→DNS 服务器”，或者从“开始→管理工具”中运行“DNS”，都会打开 DNS 服务器，用鼠标右击“正向查找区域”，在弹出的快捷菜单中选择“新建区域”命令，如图 3-47 所示。

02 在“区域类型”对话框，选择“主要区域”，如图 3-48 所示。

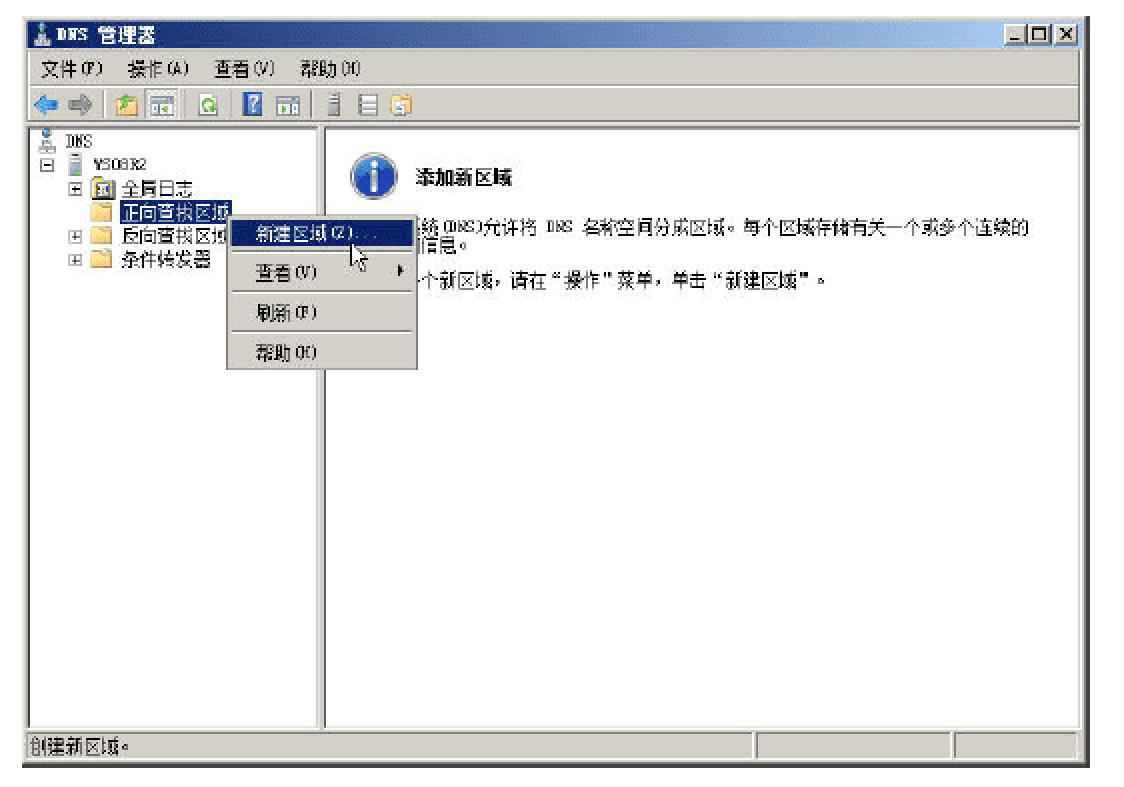


图 3-47　新建区域

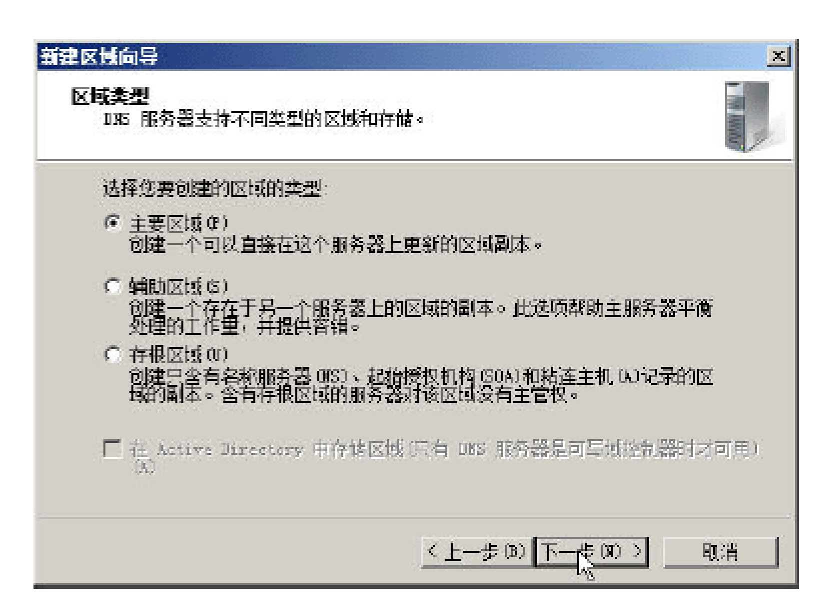


图 3-48　正向区域

03 在“区域名称”对话框，在“区域名称”文本框中输入要创建的 DNS 域名，在本例中为 msft.com，如图 3-49 所示。

04 在“区域文件”对话框中，选中“创建新文件，文件名为”单选按钮，并保持默认文件名 msft.com.dns，如图 3-50 所示。

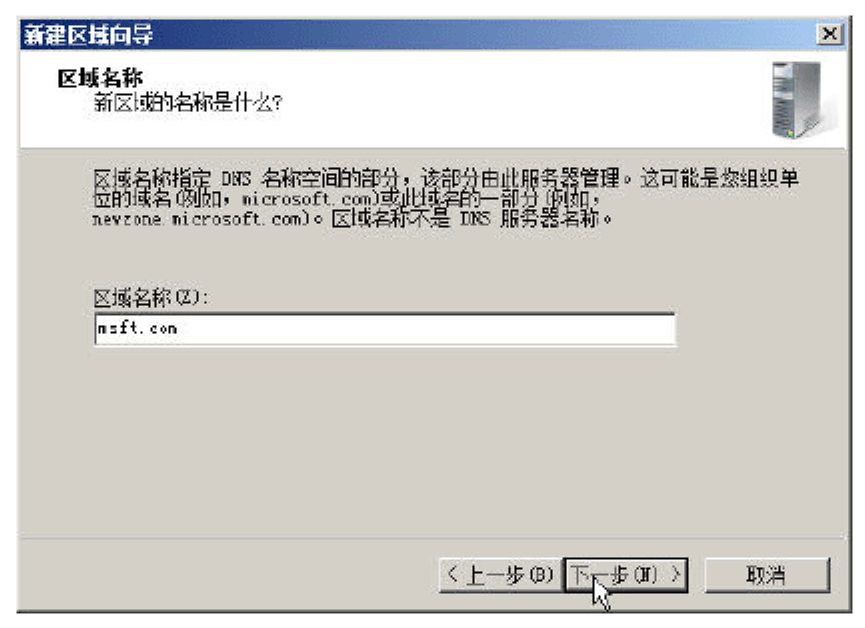


图 3-49　设置域名

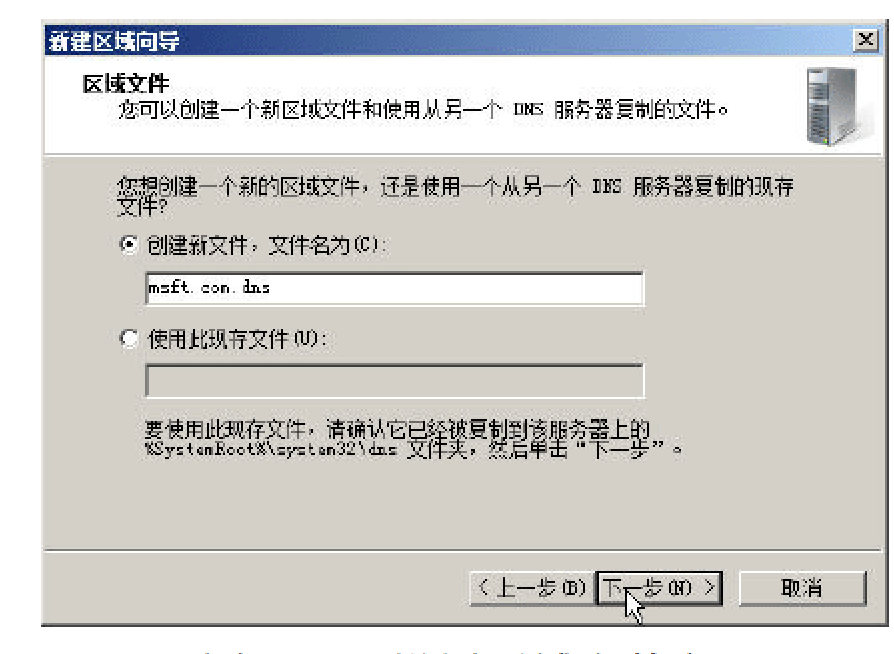


图 3-50　设置区域文件名

05 在“动态更新”对话框中选择“不允许动态更新”，如图 3-51 所示。

06 在“正在完成新建区域向导”对话框中，单击“完成”按钮，创建区域完成，如图 3-52 所示。

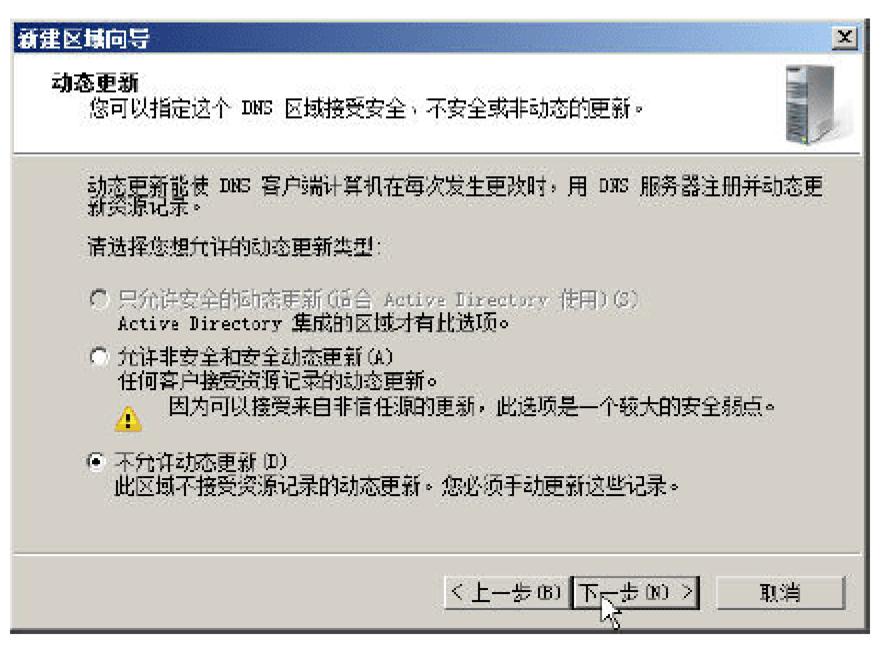


图 3-51　动态更新

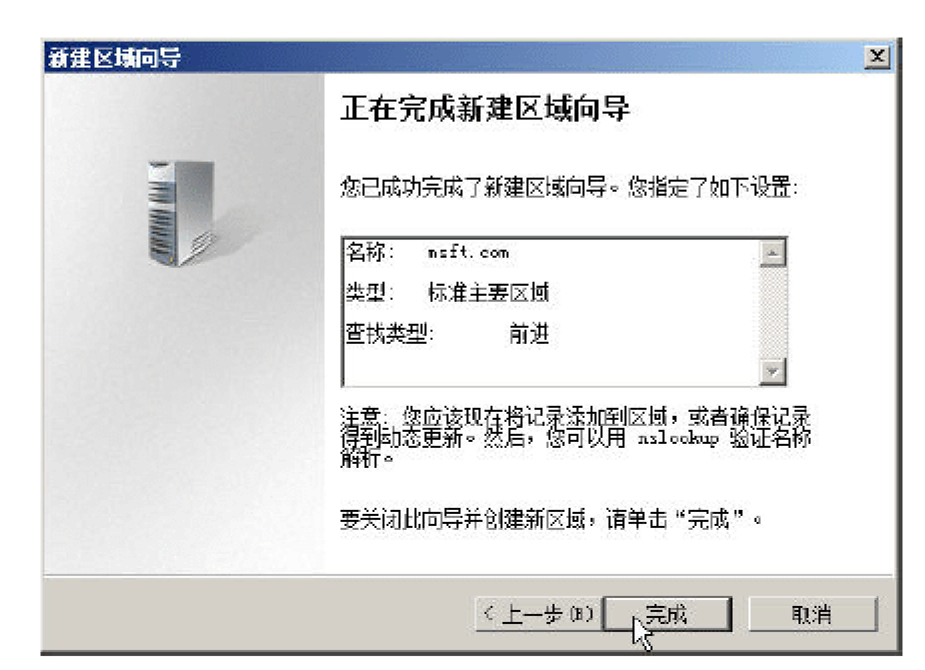


图 3-52　区域创建完成

3.6.3　在 DNS 服务器中创建记录

配置完 DNS 服务器，在与上级的 DNS 服务器地址建立联系后（只要在上级 DNS 服务器注册正确的地址），就可以对自己所属的域名（本例中为 msft.com）提供域名解析服务了。下面来介绍，在自己所属的域名中添加各种 DNS 记录的方法。

1. 创建 A 记录

Web 服务器、FTP 服务器的域名是一个 A 记录，类似于 www.sohu.com、ftp.sina.com.cn 等。A 记录在域名服务器中是最常用的，它用来把一个容易记忆的名称和一个 32 位的 IP 地址相对应。

01 打开"DNS 管理器"，定位到"msft.com"域名，在右侧的空白处，单击鼠标右键，从弹出的快捷菜单中选择"新建主机（A 或 AAAA）（S）"，如图 3-53 所示。

02 在弹出的"新建主机"对话框中，在"名称（如果为空则使用其父域名称）"文本框中输入"www"，在"IP 地址（P）"文本框中输入对应的 IP 地址"192.168.128.5"，然后单击"添加主机"按钮，如图 3-54 所示。

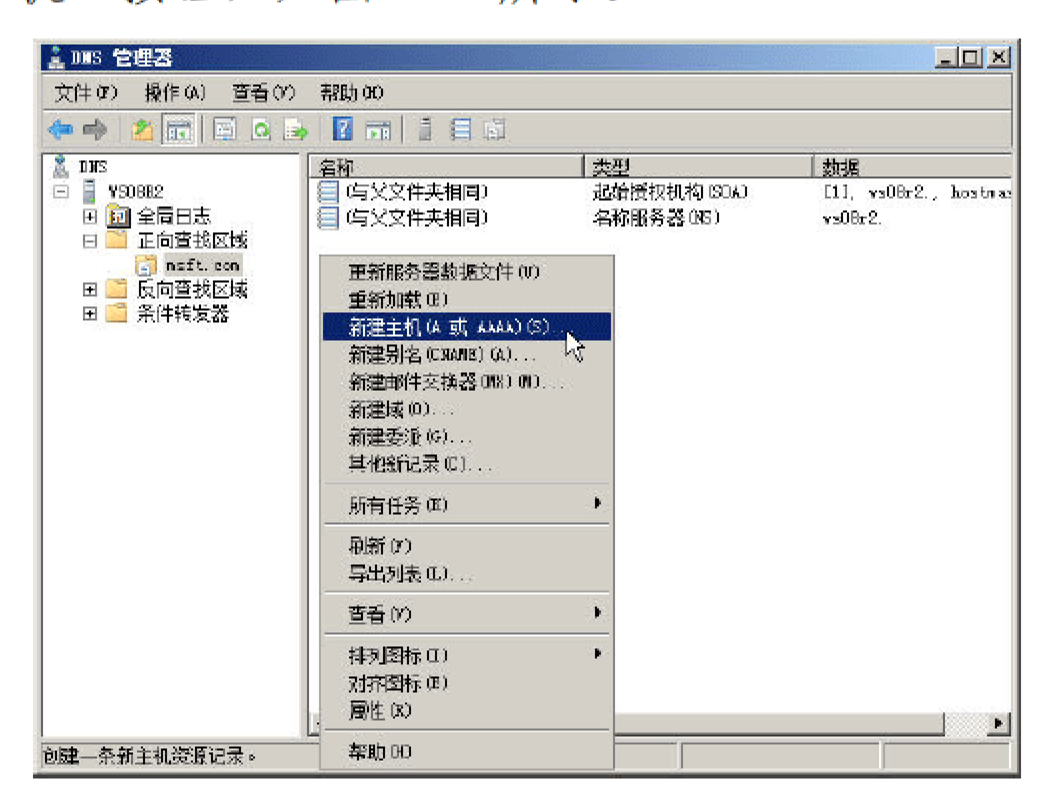


图 3-53　新建主机

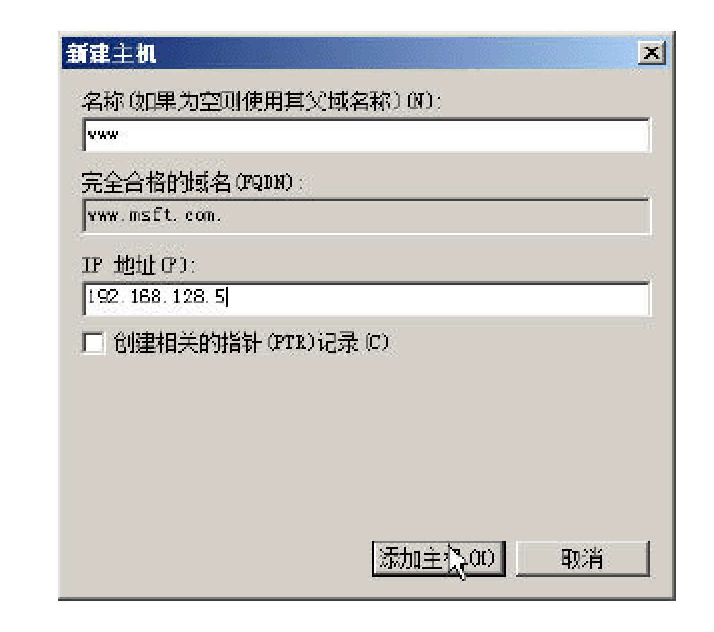


图 3-54　添加名为 www 的 A 记录

03 在弹出的"DNS"提示框中，单击"确定"按钮，如图 3-55 所示。

04 接下来，添加名为"ftp"的 A 记录，如图 3-56 所示。




图 3-55　添加主机记录完成

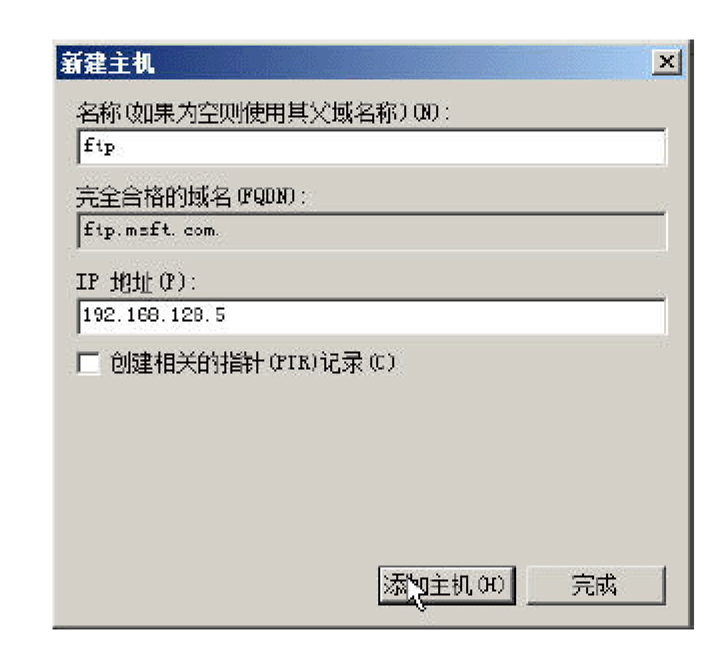


图 3-56　添加名为 FTP 的 A 记录

在创建了 www、ftp 等 A 记录之后，在 DNS 客户端解析 www.msft.com 和 ftp.msft.com 时，将能解析出对应的 IP 地址 192.168.128.5。此时，如果要解析 msft.com 中不存在的记录，如 mail.msft.com，将不会解析出 IP 地址，因为在 msft.com 区域中没有这一条记录。

2. 创建泛域名解析记录

虽然自己组建的 DNS 服务器，可以创建许多记录，但在很多情况下，创建的许多记录都是指向同一个 IP 地址.例如，在前面的例子中，名为 www、ftp 的 A 记录都指向了 192.168.128.5。如果还有其他 A 记录将要指向这台服务器（假设为朋友或者其他人提供二级域名服务并且把这些二级域名对应的网站都放在这台服务器上），在以前的情况下，应该是每增加一个需要解析的 A 记录，都要在 DNS 服务器上添加。这时候，就可以使用“泛域名解析”功能，所谓“泛域名解析”，实际上是将所有 DNS 中未明确列出的 A 记录都指向一个默认的 IP 地址，并且用星号（*）来表示。

例如，将 msft.com 的“泛域名解析”指向 192.168.128.5 的 IP 地址，只需要添加一个名称为星号（*）的 A 记录并且指向相关的 IP 地址即可，如图 3-57 所示。

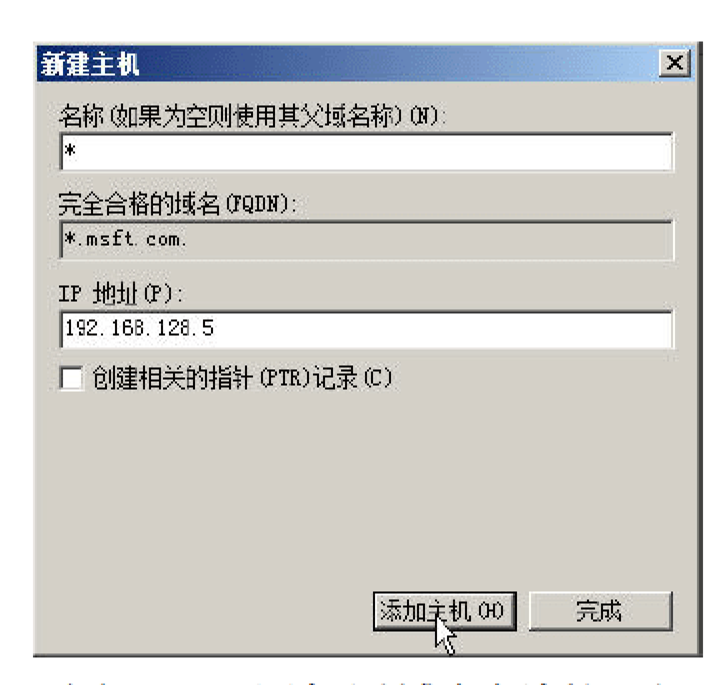


图 3-57　添加泛域名解析记录

以后，凡是在 DNS 服务器中未明确列出的名称，都会解析到 192.168.128.5。

3. 创建邮件交换器记录

邮件交换器（MX）也是一个比较重要的 DNS 记录，用来表示所属邮件服务器的 IP 地址。例如，在的域“heinfo.edu.cn”中有一个邮件服务器，其他用户（如 linnan@heuet.com）如果想给“heinfo.edu.cn”的一个邮箱（假设为 admin@heinfo.edu.cn）发信，则 linnan@heuet.com 所属的邮件服务器需要“知道”接收者邮箱（admin@heinfo.edu.cn）所属的邮件服务器的地址，这就需要查

接收者邮件（@heinfo.edu.cn）的 MX 记录，而 MX 记录就表示了邮件服务器的 IP 地址。

通常情况下，MX 记录指向一个 A 记录，而这个 A 记录将“指向”邮件服务器的 IP 地址。创建邮件交换器（MX）记录的步骤如下。

01 首先创建一个指向邮件服务器 IP 地址的 A 记录，如创建名为 mail 的 A 记录，该 A 记录指向邮件服务器的 IP 地址。

02 右击“msft.com”或者在右侧的空白窗格处单击鼠标右键，从弹出的菜单中选择“新建邮件交换器（MX）”。

03 在弹出的“新建资源记录”对话框中，如果想创建@msft.com 的邮件服务器的 MX 记录，则在“主机或子域”文本框中保留空白，在“邮件服务器的完全合格的域名（FQDN）”文本框中输入邮件服务器 IP 地址对应的 A 记录，在此可以使用 mail.msft.com，如图 3-58 所示。

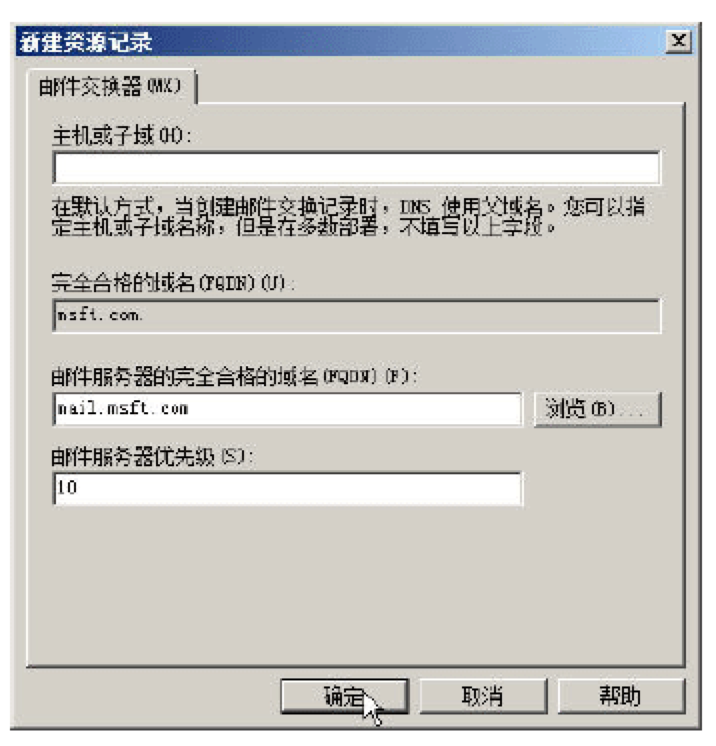


图 3-58　创建 MX 记录

许多时候，一个域中的邮件服务器不止一台。例如，本节中，在 IP 地址 192.168.128.5 的邮件服务器上创建所有后缀为@msft.com 的邮箱。如果想再创建第 2 台邮件服务器，使用后缀为@vip.msft.com，在 IP 地址为 192.168.128.6 的计算机上，则应该先创建一个 A 记录，如 mailserver.msft.com，在创建 MX 记录时创建子域并且使用刚刚创建的 A 记录，如图 3-59 和图 3-60 所示。

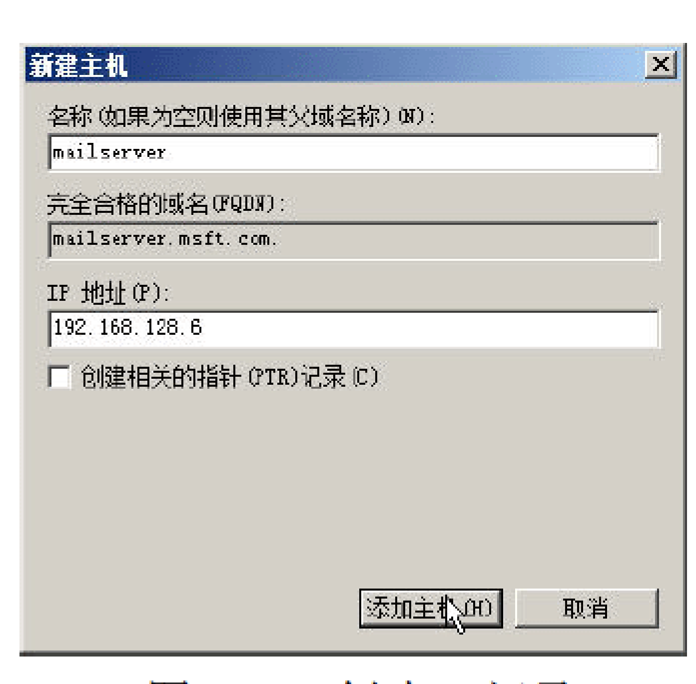


图 3-59　创建 A 记录

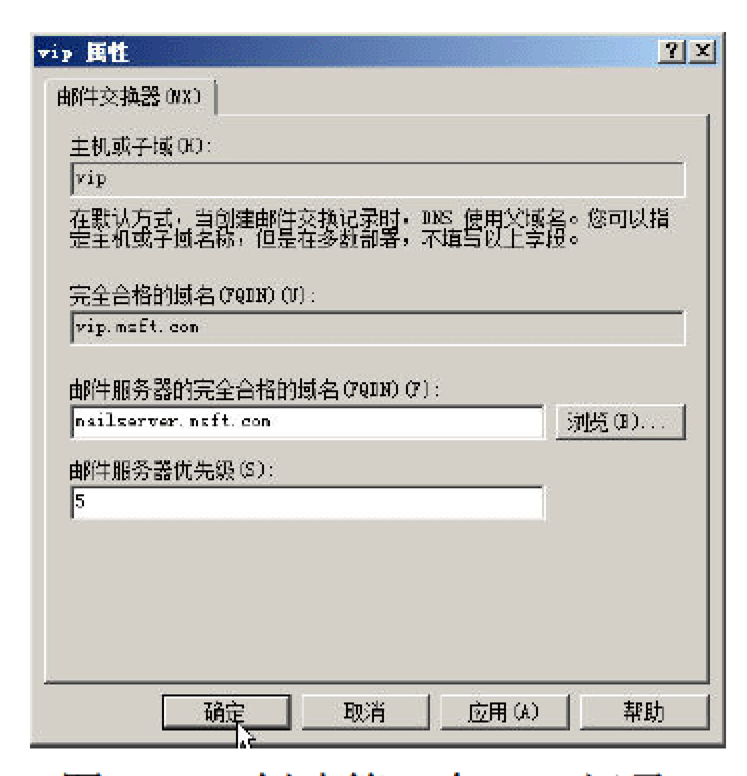


图 3-60　创建第 2 个 MX 记录

在图 3-60 所示对话框中，在“邮件服务器优先级”文本框中，设置邮件服务器的优先级。数

字越小，优先级越高，在本例中，设置数字为 5。

4. 创建其他记录

在 DNS 服务器中，还可以创建其他记录，如别名记录（CNAME）、IPv6 主机记录（AAAA）、服务位置记录（SRV）等。如果需要创建这些记录，可以在 DNS 服务器中，在右侧的空白窗格中单击鼠标右键，从弹出的快捷菜单中选择“其他新记录”，并在弹出的“资源记录类型”文本框中，选择相应的记录，然后选择“创建记录”即可，如图 3-61 和图 3-62 所示。

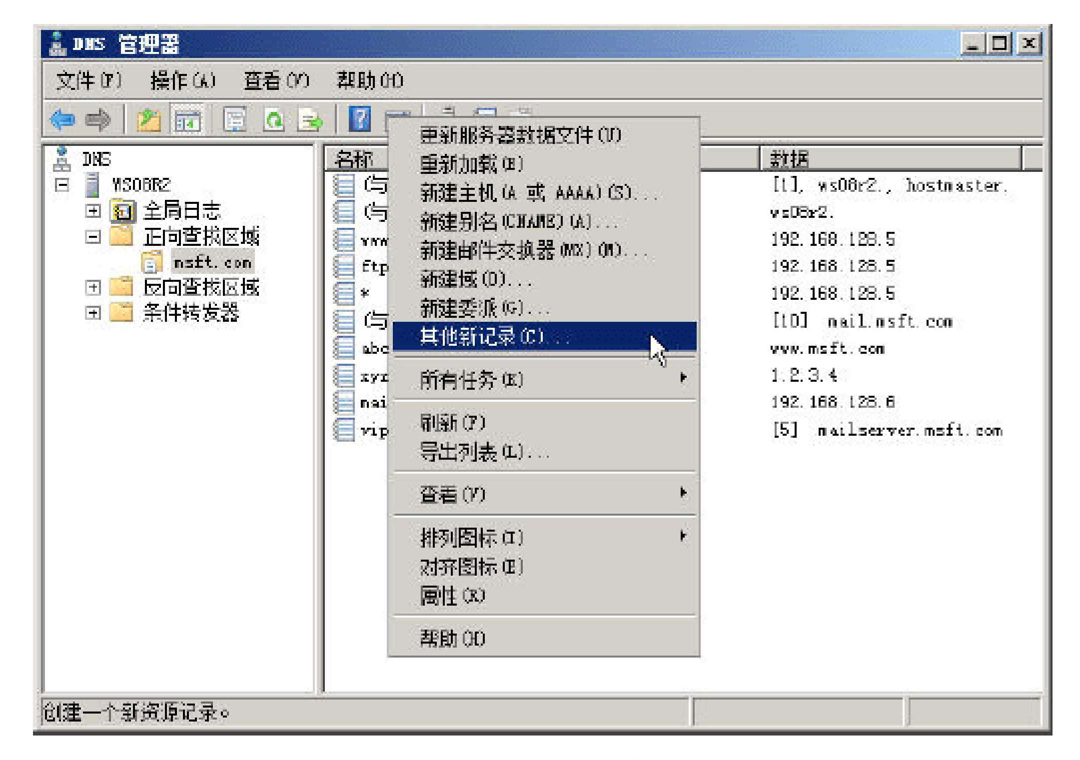


图 3-61　创建其他新记录

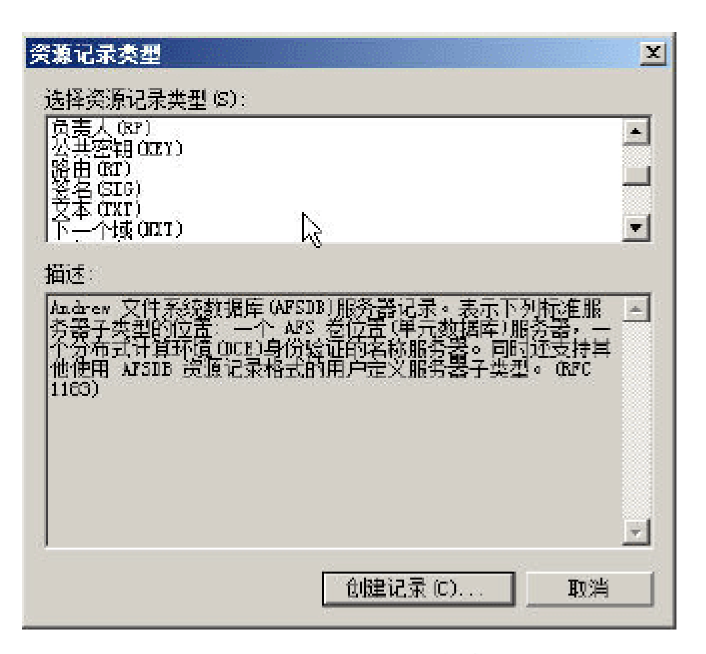


图 3-62　选择其他记录

如图 3-63 所示，是创建 CNAME 记录。这些记录的使用并不是很多，在此不做详细的介绍。

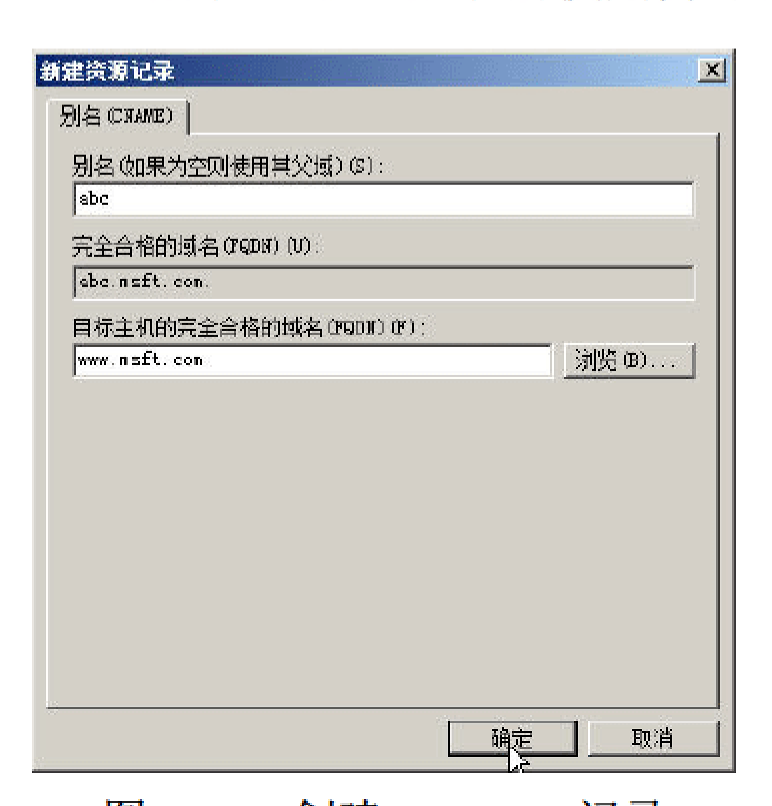


图 3-63　创建 CNAME 记录

3.6.4　使用 nslookup 命令检查 DNS 信息

如果要对 DNS 服务器排错，或者想要检查 DNS 服务器的信息，可以使用 nslookup 命令。在网络中的任何一台工作站上，在命令提示符下输入 nslookup 命令，然后按回车键。下面介绍使用 nslookup 检查 DNS 信息的方法。

（1）如果想设置 nslookup 使用的 DNS 服务器，可以输入 server DNS_server_ip 并按回车键。

（2）如果想检查某个 DNS 域名的 MX 记录，可以先输入 set q=mx，然后输入想要检查的 DNS 域名，如 msft.com，输入之后，将显示 DNS 服务器的 MX 记录及对应的 IP 地址，如图 3-64 所示。

（3）如果要显示其他记录，则输入 set q=any，然后输入想要查询的记录的名称，如 www.msft.com，如图 3-65 所示。

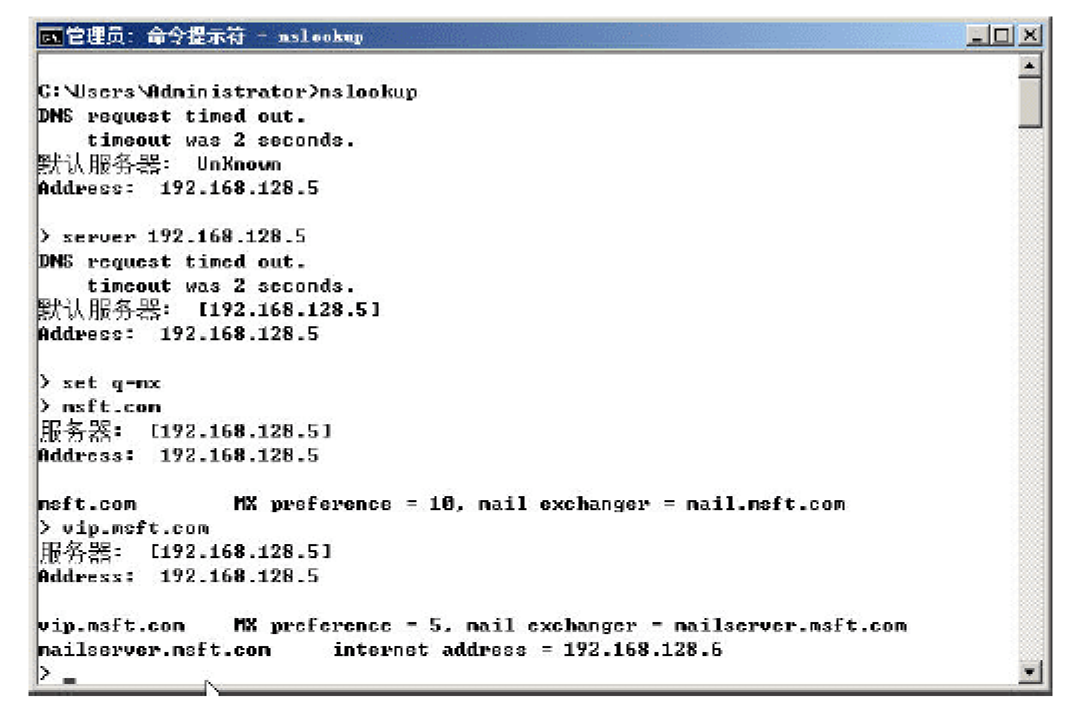


图 3-64　显示 MX 记录

```
> set q=any
> www.msft.com
服务器:  UnKnown
Address:  192.168.128.5

www.msft.com    internet address = 192.168.128.5
> xyz.msft.com
服务器:  UnKnown
Address:  192.168.128.5

xyz.msft.com    internet address = 1.2.3.4
> _
```

图 3-65　检查其他记录

（4）如果要退出 nslookup 命令，输入 exit。

3.6.5　组建内部 DNS 覆盖公网 DNS 解析结果

DNS 服务器配置虽然简单，但如果用的好，可以解决一些“疑难”问题。下面通过例子进行说明。

某单位通过光纤连接到 Internet，网通公司提供了 5 个 IP 地址，其中 1 个 IP 地址用于 Internet 接入，1 个 IP 地址作为网站服务器，并且这个公网地址映射到内网的 Web 服务器（FTP 服务器同时也在这台机器上），1 个 IP 地址作为邮件服务器映射到另一台内网服务器上。该单位申请的域名为 heuet.org。现在问题是：外面的用户可以使用 www.heuet.org 和 mail.heuet.org 登录单位的网站和邮箱，但单位内部的人却不能通过 www.heuet.org 和 mail.heuet.org 来访问单位的网站和邮件系统。

本案例中，路由器启用了 NAT 功能，并且使用 202.206.198.194 共享上网，将 202.206.198.195 映射到内网的 192.168.1.5 的 Web 服务器中，网络拓扑如图 3-66 所示。

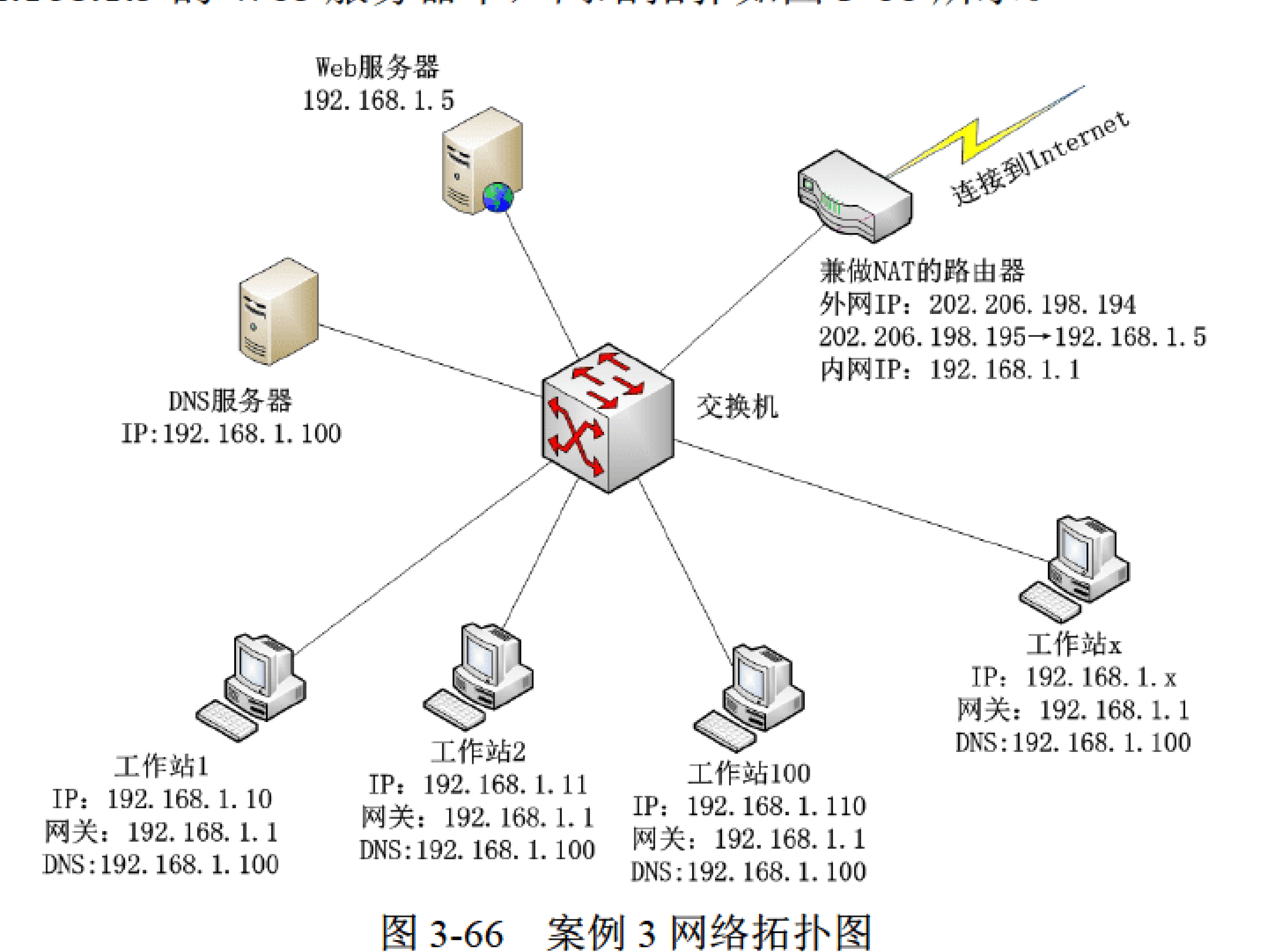


图 3-66　案例 3 网络拓扑图

本案例中，在 192.168.1.5 的服务器中，保存了 www.heuet.org 网站（同时提供了 ftp.heuet.org 的 FTP 服务，用来上传和更新网站），heuet.org 域名在域名服务商处进行了注册，并且将 www 等 A 记录注册到 202.206.198.195 的 IP 地址中（如图 3-67 所示）。这样，当工作站尝试（如 192.168.1.10 的工作站）访问 www.heuet.org 时，解析的地址是 202.206.198.195，但许多路由器不支持从内网访问 202.206.198.195 并且将此地址再映射到 192.168.1.5 中，所以不能访问网站；但外网用户是直接通过 202.206.198.195 访问，路由器将对此地址的访问转发到 192.168.1.5，因此是可以访问的。



图 3-67　heuet.org 的 DNS 服务器中 A 记录指向的地址

在这种情况下，一般的解决方法是在 heuet.org 中注册内网的地址如 www2，并将 www2 解析为内网地址 192.168.1.5，让内网用户访问 www2.heuet.org，就可以访问 Web 网站了，如图 3-68 所示。



图 3-68　添加到内网地址的 A 记录

这样，内网用户不需要修改其 DNS 服务器，即可以完成网站的访问。但一些不熟悉计算机的用户，不明白为什么在单位内网访问网站是使用 www2.heuet.org，而在单位外面是使用

www.heuet.org 进行访问。这时候，就需要采用另外一种办法了。

对于本案例来说，如果想让内、外网用户访问网站都使用同一种方式来访问，则需要在内网组建 DNS 服务器，创建内网的 heuet.org 区域，将 www 和 ftp 等 A 记录解析成内网的地址，并且让所有工作站的 DNS 指向新创建的 DNS 服务器，在 DNS 服务器上启用“转发器”转发所有 heuet.org 以外的域名解析需求。本案例的解决步骤如下。

01 在内网的一台服务器（本例中，这台服务器的 IP 地址是 192.168.1.200）中，安装 Windows Server 2003 和 DNS 服务。

02 参照 3.6.2 节，创建名为 heuet.org 的区域，并添加 DNS 转发器地址。不同之处如图 3-69 所示。

03 参照 3.6.3 节，创建名为 www 和 ftp 的 A 记录，并且其 IP 地址为 192.168.1.5，如图 3-70 和图 3-71 所示。

04 网络中所有的工作站，其 DNS 服务器地址都配置为 192.168.1.200，如图 3-72 所示，这是 IP 地址为 192.168.1.5 的工作站的 TCP/IP 配置信息。

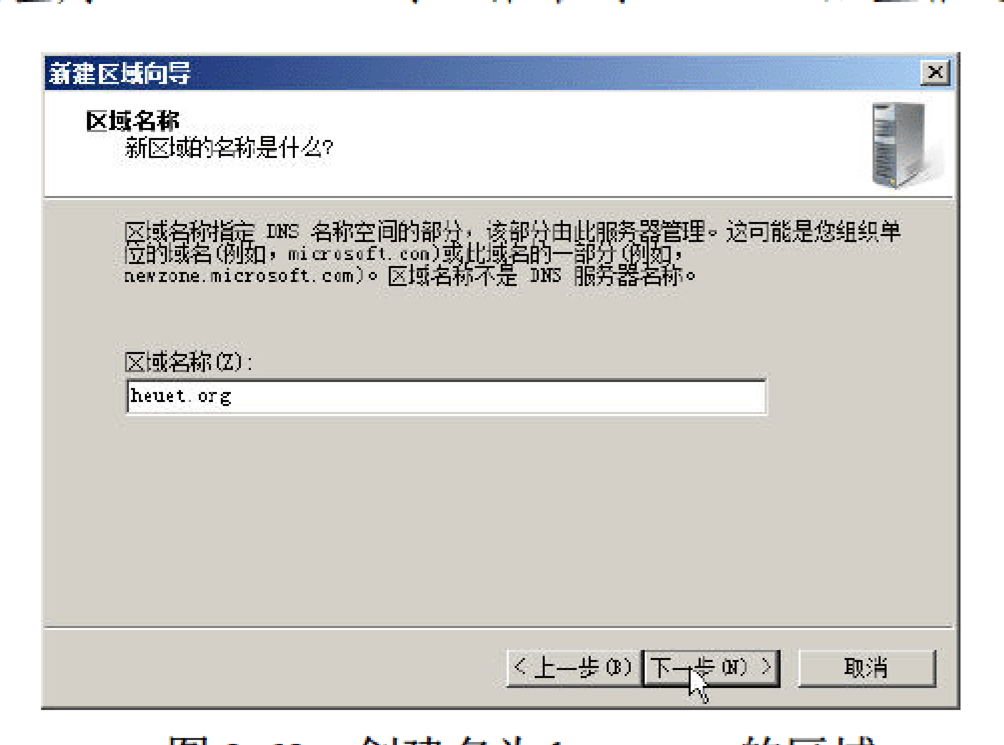


图 3-69　创建名为 heuet.org 的区域

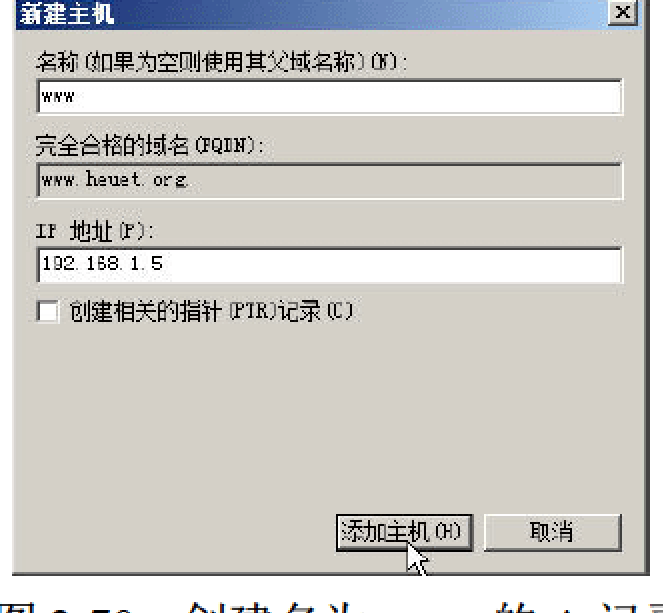


图 3-70　创建名为 www 的 A 记录

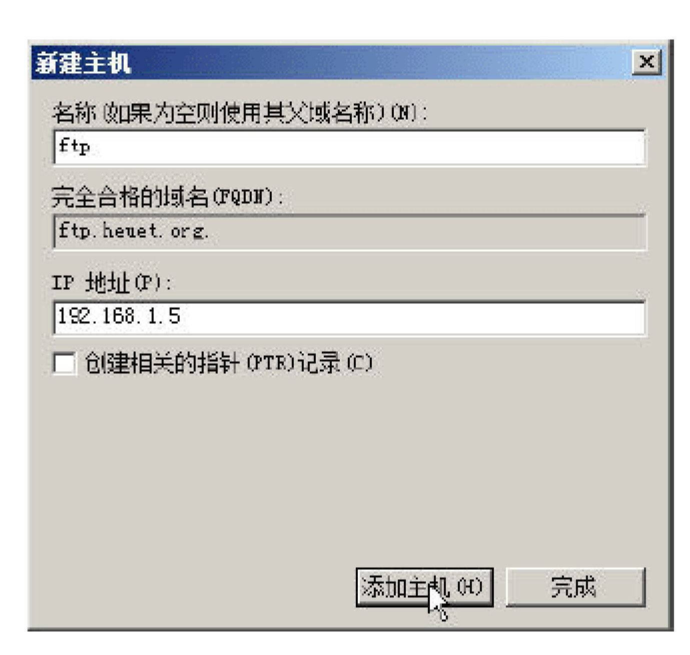


图 3-71　创建名为 ftp 的 A 记录

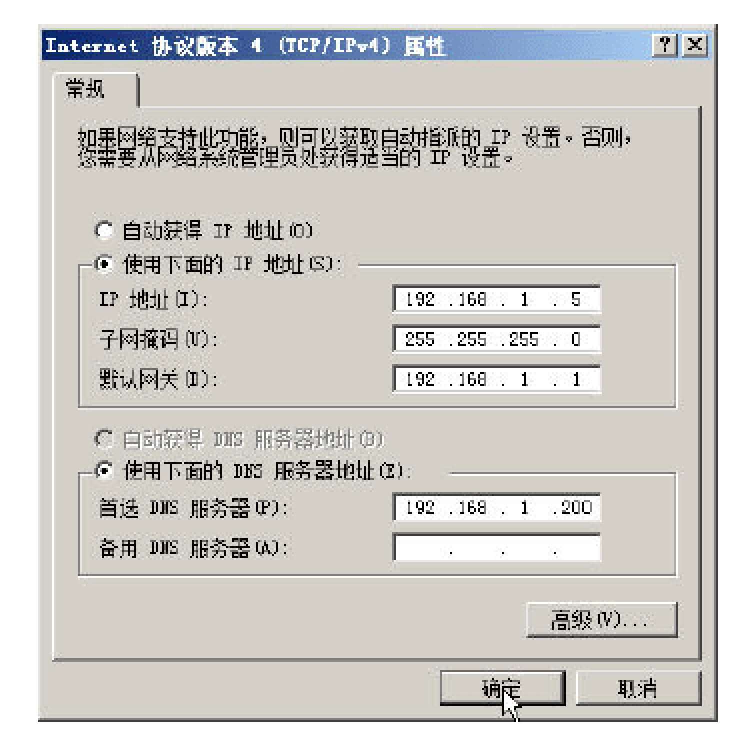


图 3-72　某台工作站的 TCP/IP 配置



说 明

如果 Web 服务器是 Windows Server 2003，也可以在 Web 服务器上安装 DNS 服务器，这样，网络中所有工作站的 DNS 都配置为 192.168.1.200 即可，其他的设置和步骤 1～3 相同。

3.7　WINS 服务器的安装和配置

WINS 是“Windows Internet 名称服务”的简称，它提供了动态复制数据库服务，此服务可以将 NetBIOS 名称注册并解析为网络上使用的 IP 地址。Microsoft Windows Server 家族提供了 WINS，它运行服务器计算机来充当 NetBIOS 名称服务器并注册和解析网络上启用 WINS 的客户端计算机名称。简单来说，WINS 服务器解析诸如 aaa、bbb 等计算机的“短名称”，DNS 服务器解析诸如 aaa.bbb.ccc 等之类的“长名称”。所以，WINS 服务主要用于局域网，而 DNS 服务可以在任何 Internet 网络中使用。

3.7.1　安装 WINS 服务器

在 Windows Server 2008 中，选择“服务器管理器→功能→添加功能”，添加 WINS 服务器，如图 3-73 所示。



图 3-73　添加 WINS 服务

添加之后，不需要重新启动计算机，WINS 服务器即可以使用。在图 3-73 所示的“选择功能”对话框中，还可以添加 TFTP 客户端（大家常用的 telnet 命令）、BitLocker 驱动器加密等功能。

WINS 服务器的配置相对来说比较简单，在大多数情况下，都不需要配置，只要在客户端指定 WINS 服务器，客户端就会把自己的 NetBIOS 名称和 IP 地址在 WINS 服务器中注册，其他客户端也就能在 WINS 服务器查找 NetBIOS 名称的 IP 地址并用于网络通信。

3.7.2　在 WINS 服务器中添加静态映射

通常情况下，WINS 客户端会将自己的计算机名称和 IP 地址在 WINS 服务器上进行注册。当有些计算机不能在 WINS 服务器中注册时，要想让其他客户端使用 NetBIOS 名称进行网络通信，必需在 WINS 服务器中通过添加静态映射的方法，添加 NetBIOS 名称和 IP 地址的对应关系，步骤如下。

01 进入 WINS 服务器，定位到“计算机名→活动注册”，用鼠标右键单击“活动注册”，在弹出的菜单中选择“新建静态映射”命令，如图 3-74 所示。

02 在弹出的“新建静态映射”对话框中，在“计算机名称”文本框中，输入某台计算机的 NetBIOS 名称，在“类型”下拉列表中选择“惟一”，在“IP 地址”文本框中，输入此台计算机对应的 IP 地址，然后单击“确定”按钮，如图 3-75 所示。

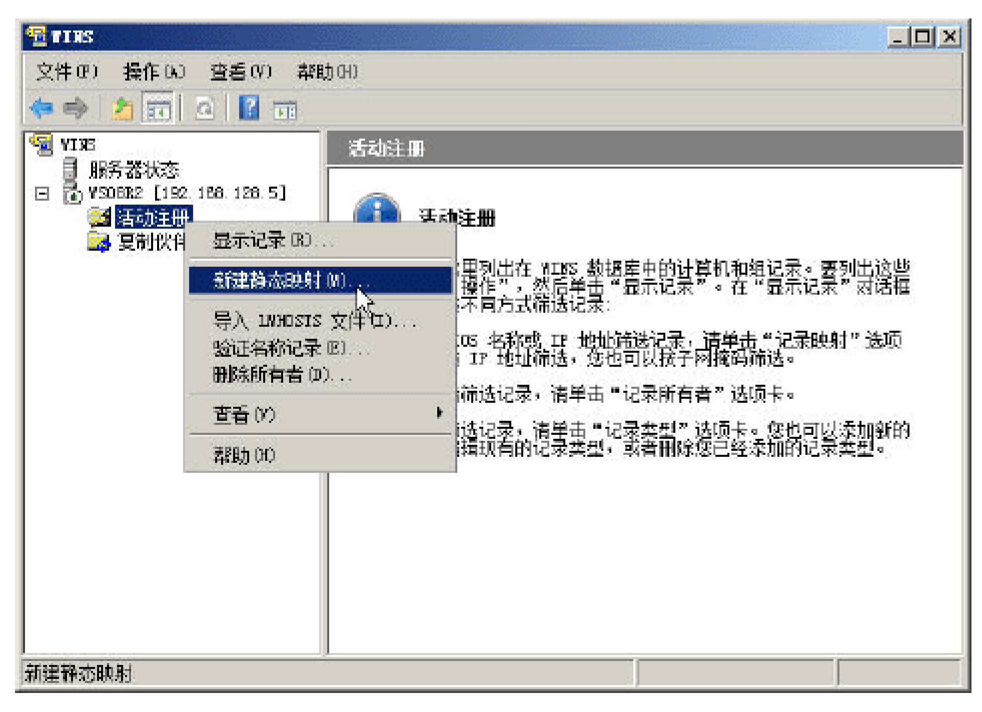


图 3-74　新建静态映射

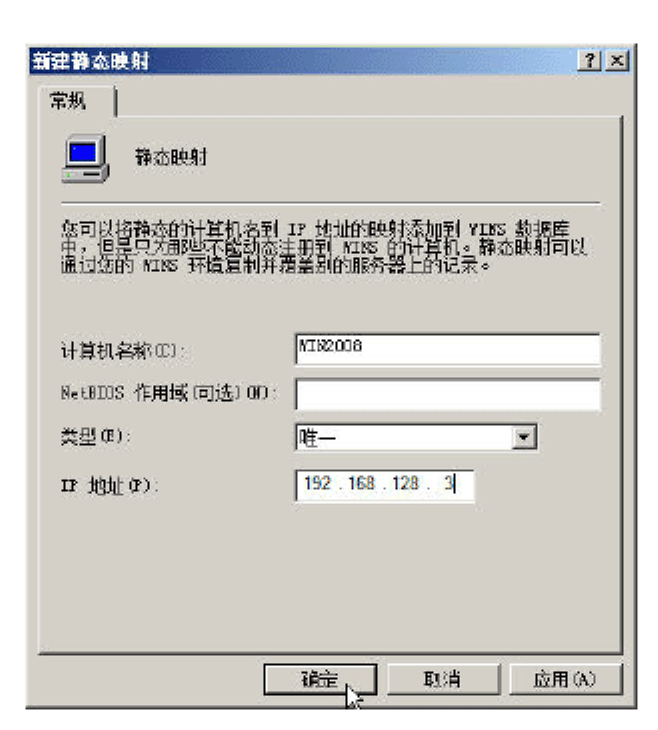


图 3-75　创建静态映射

3.7.3　导入包括静态项的文件

如果有大量的计算机需要添加为静态映射，可以用“记事本”编辑一个文本文件，然后使用“导入 LMHOSTS 文件”的方式，批量导入这些文件。LMHOSTS 文件的格式如下：

```
192.168.1.1      hostserver
192.168.1.98     server23
192.168.3.55     mailserver
```

这和 DNS 的 hosts 文件相类似，前面是 IP 地址，后面是 NetBIOS 名称。然后将上述信息保存为 LMHOSTS 文件，在 WINS 服务器上用鼠标右键单击“活动注册”，在弹出的快捷菜单中选择“导入 LMHOSTS 文件”（如图 3-75 所示），在后面的步骤中选择要导入的文本文件即可。

3.7.4　查看 WINS 服务器中的注册信息

在 WINS 服务器中可以查看在 WINS 服务器中所有的注册信息，包括工作站自动在 WINS 服务器注册的信息和在 WINS 服务器中通过静态映射指定的信息，方法如下：

01 在 WINS 服务器中，定位到“计算机名→活动注册”，用鼠标右键单击，从弹出的菜单中选择“显示记录”，如图 3-76 所示。

02 在弹出的“显示记录”对话框中，默认出现“记录映射”选项卡，如图 3-77 所示。





图 3-76　显示 WINS 服务器记录

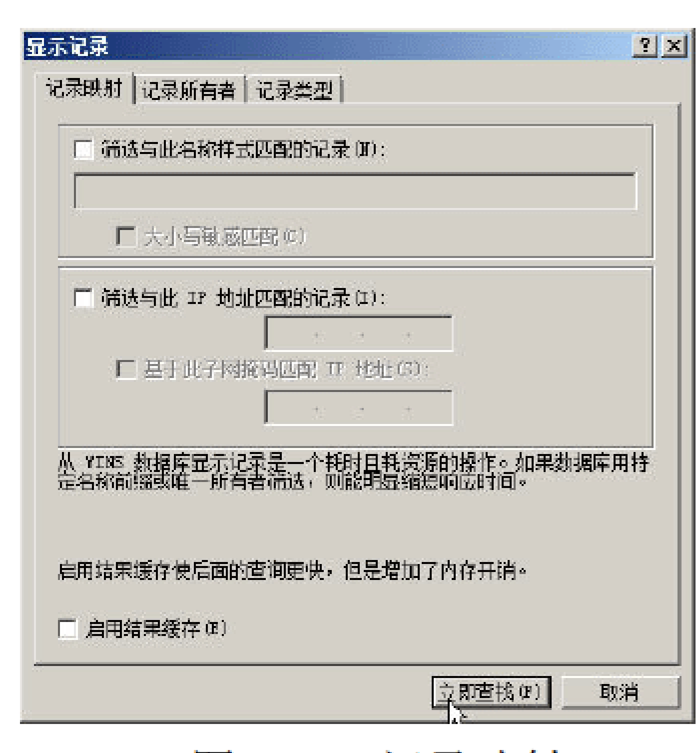


图 3-77　记录映射

“记录映射”选项卡中包含 3 个选项组，分别介绍如下。

- 如果选中“筛选和此名称样式匹配的记录”，则在下面输入在 WINS 数据库中搜索的计算机 NetBIOS 名称。如果同时选中“大小写敏感匹配”，按提供的匹配条件（包括大写）执行记录搜索。
- 如果选中“筛选和此 IP 地址匹配的记录”，则在此处输入在 WINS 数据库中搜索的 IP 地址。如果同时选中“基于此子网掩码匹配 IP 地址”，则在此处输入子网掩码进一步筛选 IP 地址搜索。
- 如果选中“启用结果缓存”，结果缓存允许 WINS 名称记录所有者的记录下载到本地计算机上，在记录集上随后的查询操作过程中提供更高的性能。返回到本地计算机的记录集存储在本机内存中。当记录集存储在内存中时，本地计算机的性能可能会受到影响，这依赖本机内存的数量和记录集的大小。

03 在“记录所有者”选项卡中，指定为哪些所有者显示记录，如图 3-78 所示。

04 在“记录类型”选项卡中，列出在筛选 WINS 数据库视图时可用的 NetBIOS 名称类型。默认情况下，在筛选器掩码中包含了全部的名称类型。对于不想查看的名称类型，单击以从当前筛选的视图中清除或删除它们。设置之后，单击“立即查找”按钮即可，如图 3-79 所示。

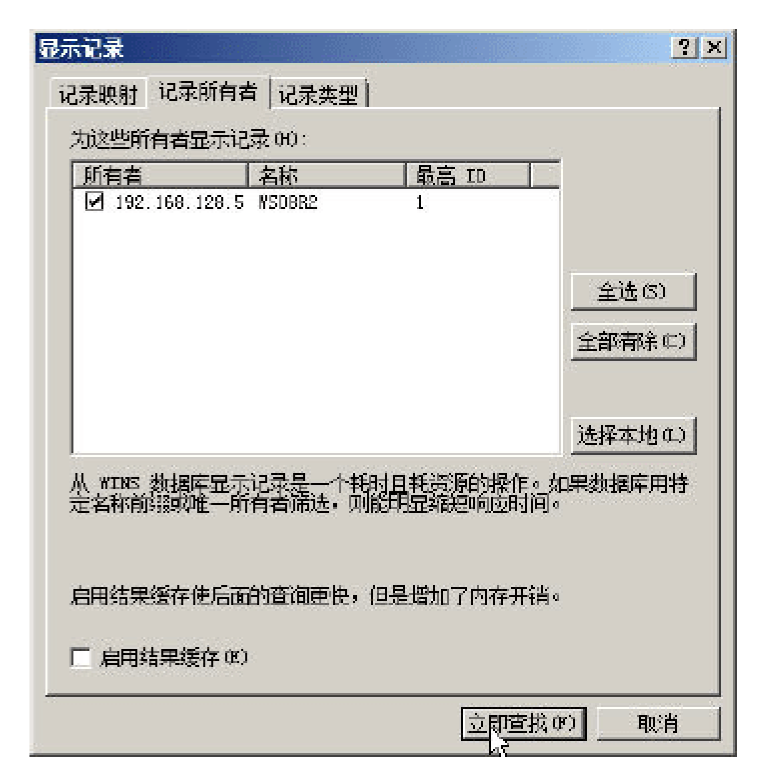


图 3-78　记录所有者

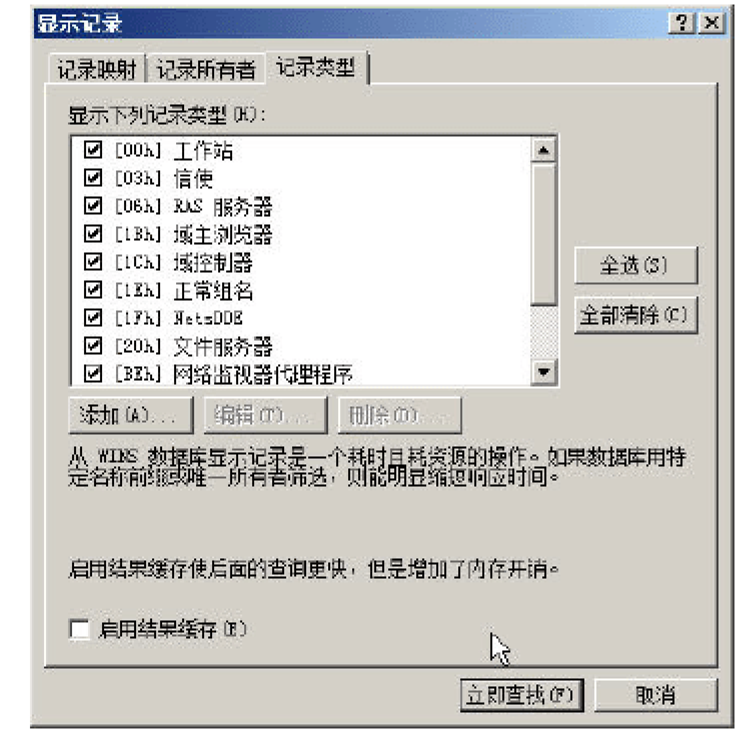


图 3-79　记录类型

05 查找完成后，在 WINS 服务器中的注册信息会在“活动注册”右侧窗口中显示，如图 3-80

所示。



图 3-80　当前 WINS 服务器的注册信息



说 明

在“静态”标题中，有“叉号”标记的，表示静态映射，没有此标志的，是动态映射。

3.8　WINS 工作站的设置

在工作站中使用 WINS 服务器是比较简单的事情：如果工作站从网络中的 DHCP 服务器获得地址，则在 DHCP 服务器为“作用域选项”或“服务器选项”指定 WINS 服务器的地址及类型即可；如果工作站手动指定 IP 地址，则手动添加 WINS 服务器的地址即可。现在分别介绍这两种情况。

3.8.1 在 DHCP 服务器中分配 WINS 服务器

如果网络中使用 DHCP 服务器为工作站分配 IP 地址，在创建作用域的同时，可以一同指定 WINS 服务器的地址，或者在配置“服务器选项”中，一同为所有作用域指定 WINS 服务器地址及类型。例如，在 DHCP 服务器的“服务器选项”对话框中，在 DHCP 服务器中添加 WINS 服务器的地址 192.168.1.10，并添加节点类型为 0x8，如图 3-81 和图 3-82 所示。

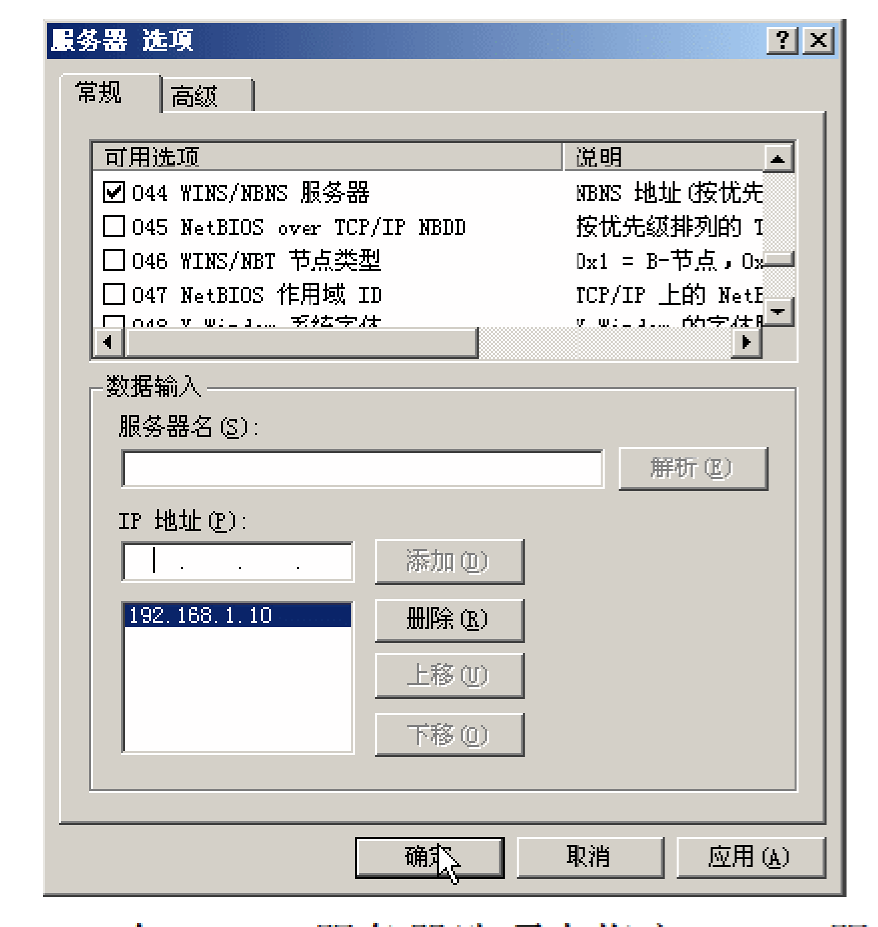


图 3-81　在 DHCP 服务器选项中指定 WINS 服务器地址

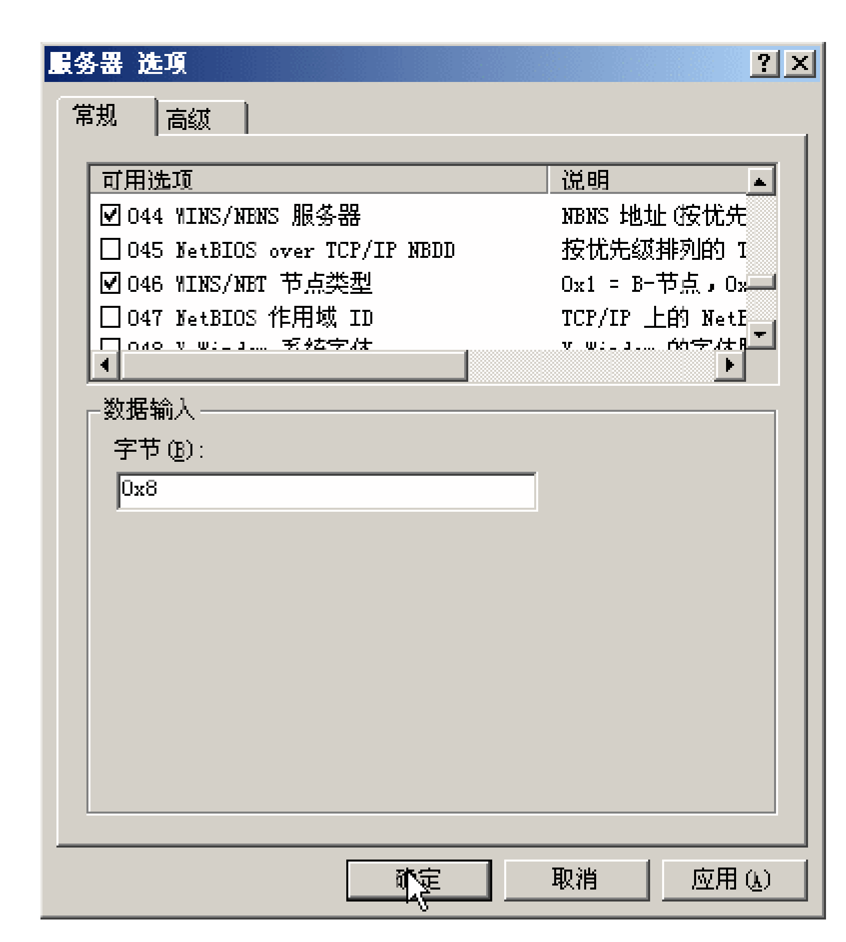


图 3-82　指定 WINS 服务器类型

3.8.2　工作站的配置

在网络中，工作站的配置是很简单的，只要指定 WINS 服务器的地址即可。如果网络中使用 DHCP 服务器分配地址并且指派了 WINS 服务器的地址和节点类型，工作站只要设置为自动获得地址即可得到正确的网络参数。为工作站指定 WINS 服务器的操作步骤如下。

01 在工作站（或需要指定 WINS 服务器地址的服务器上），打开网络连接属性，在设置 TCP/IP 地址的对话框，单击“高级”按钮，如图 3-83 所示。

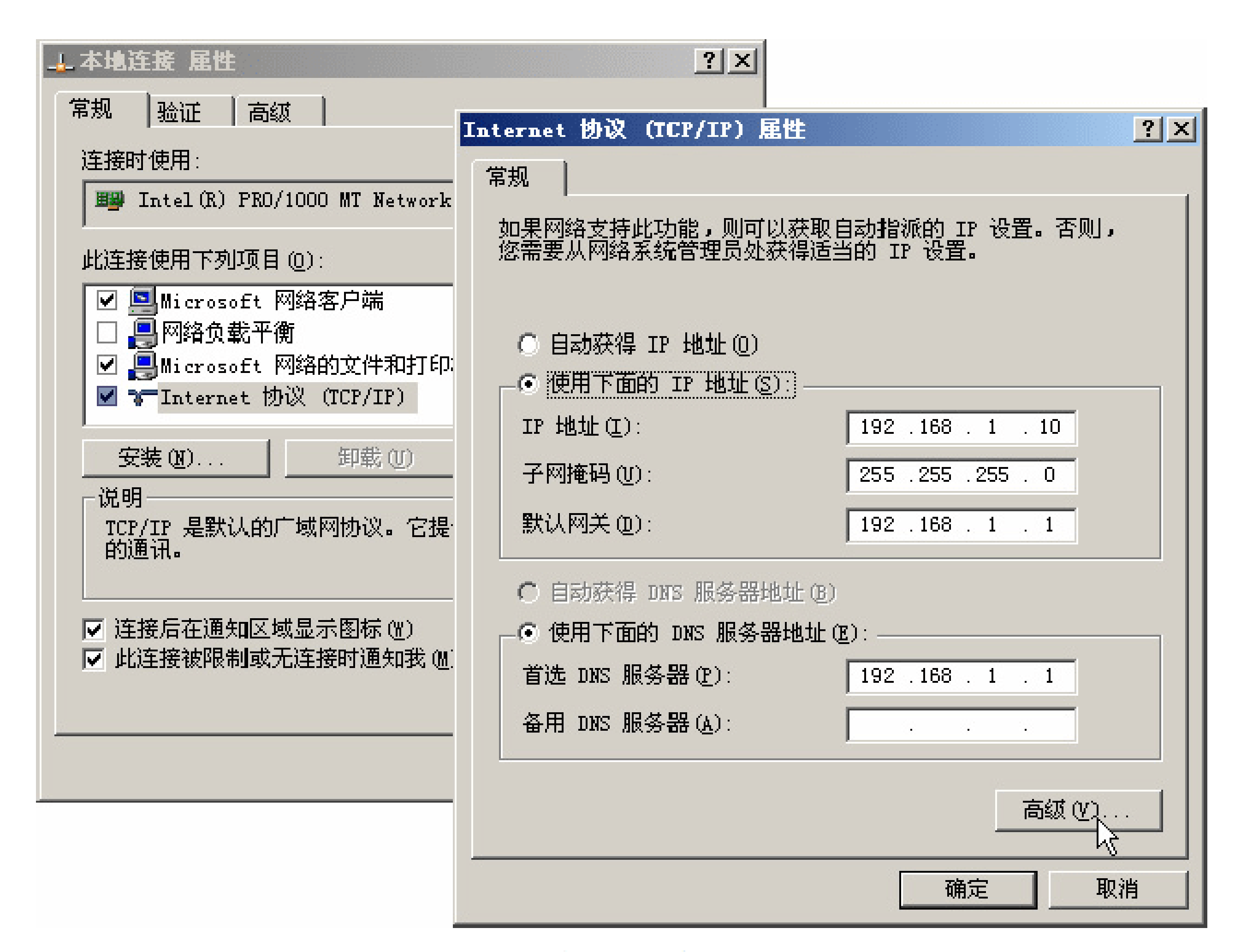


图 3-83　单击“高级”按钮

02 在打开的“高级 TCP/IP 设置”对话框中，进入“WINS”选项卡，单击“添加”按钮，如图 3-84 所示。

03 在弹出的对话框中，输入 WINS 服务器的地址，然后单击“添加”按钮，如图 3-85 所示。

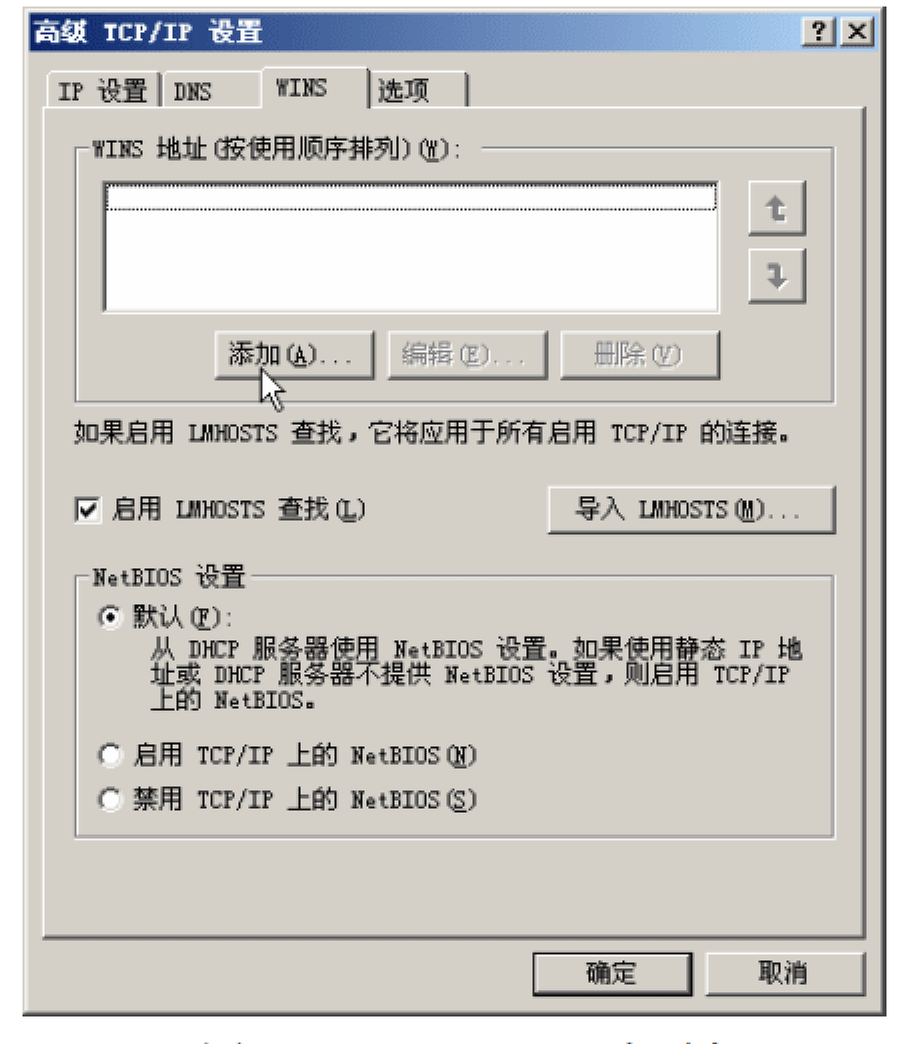


图 3-84　“WINS”选项卡



图 3-85　添加 WINS 服务器

04 添加之后，单击“确定”按钮。

3.8.3　在自动获得 IP 地址的工作站上进行验证

如果网络中使用 DHCP 服务器，只要设置“自动获得 IP 地址”和“自动获得 DNS 服务器地址”即可，如图 3-86 所示。

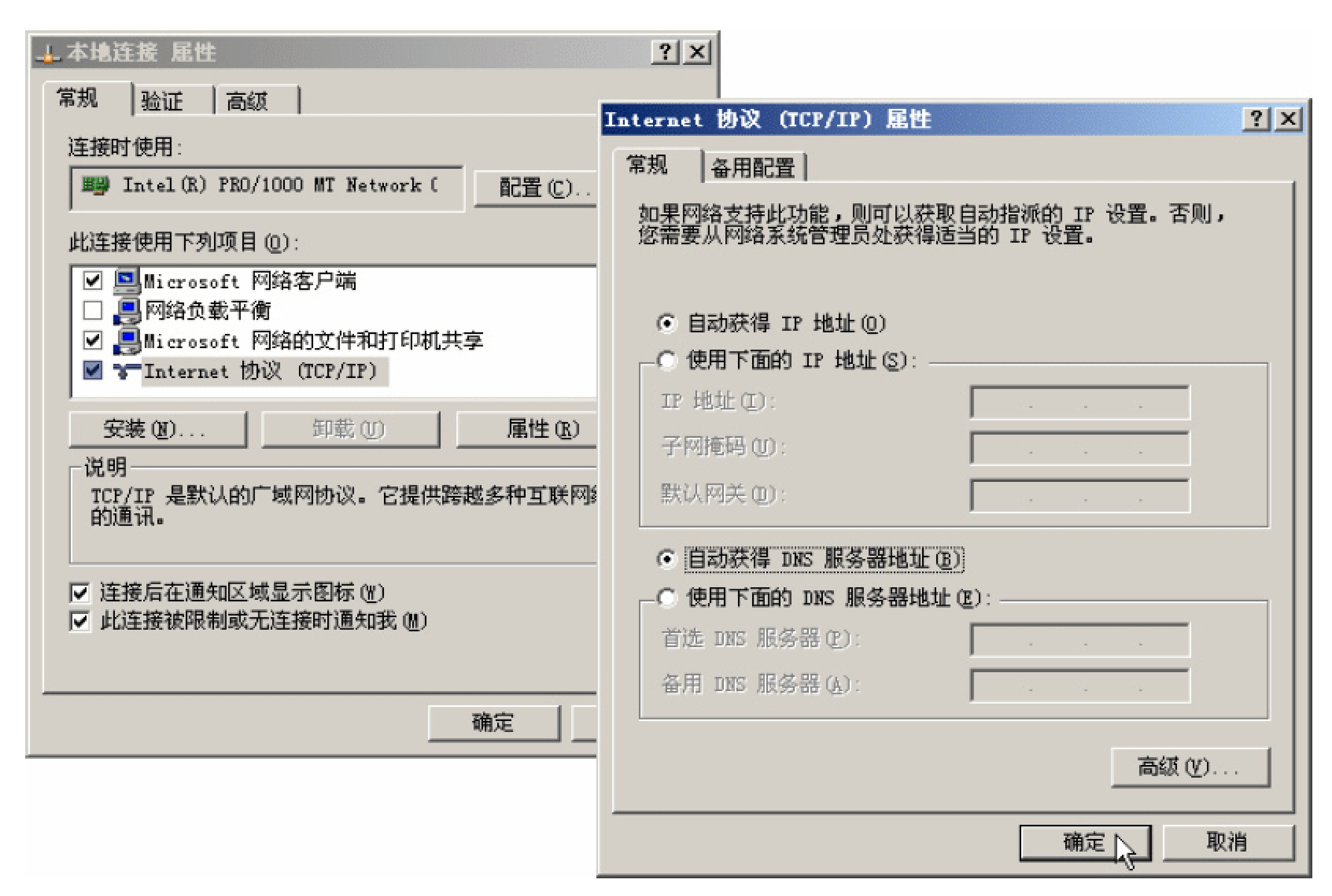


图 3-86　自动获得 IP 地址和 DNS 服务器地址

在工作站上，可以在命令提示窗口中，使用“ipconfig/all”命令，查看 WINS 服务器、DNS 服务器地址等参数，如图 3-87 所示。

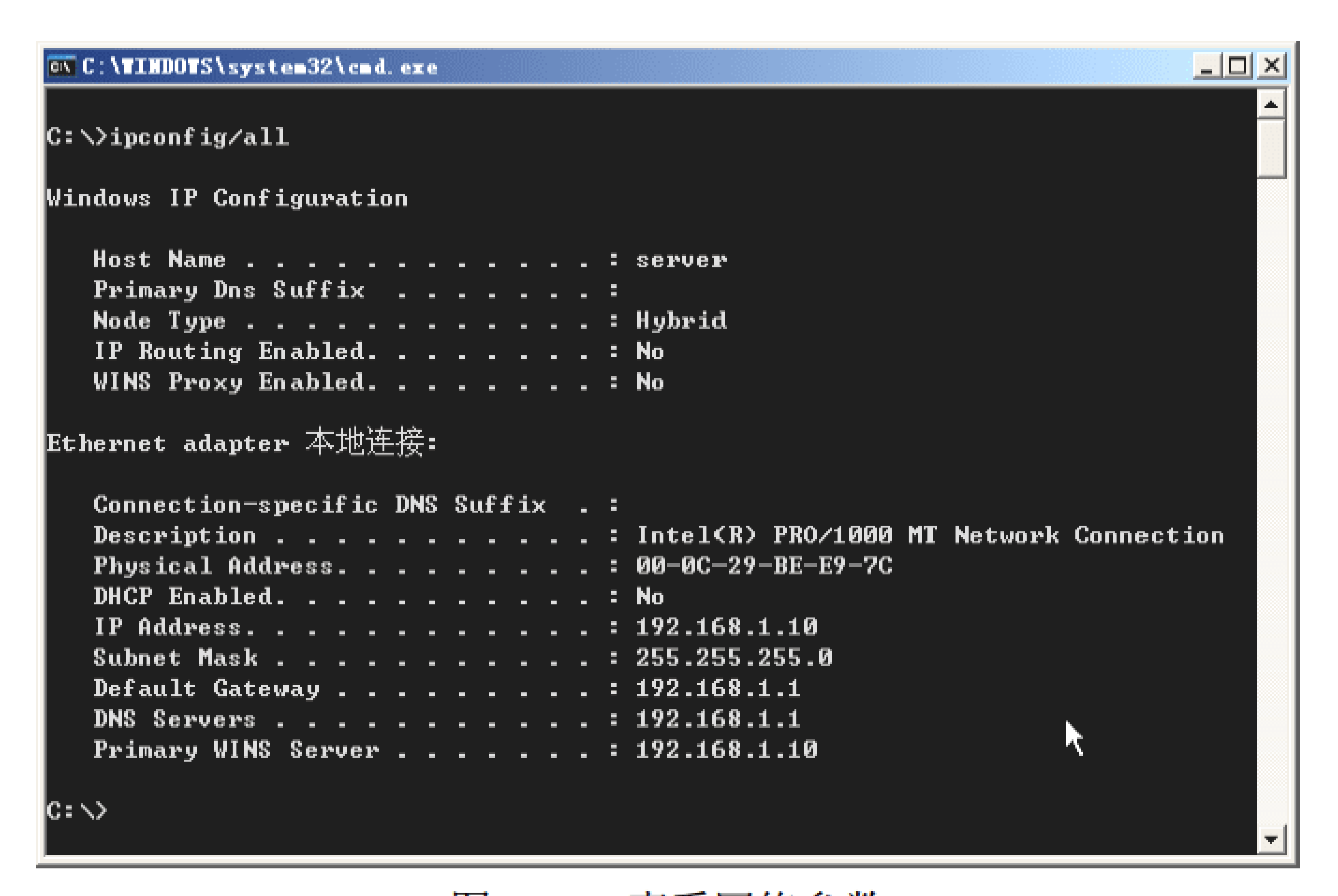


图 3-87　查看网络参数

在图 3-87 中，在“DNS Servers”后面列出的是 DNS 服务器地址，在“Primary WINS Server”后面列出的是 WINS 服务器的地址。

3.8.4　WINS 应用示例

某企业使用的是 Symantec 企业版防病毒软件，这个单位有 5 个 VLAN，在部署 Symantec 之后，发现只有和 Symantec 服务端在同一 VLAN 的客户端才能升级补丁，而其他 VLAN 的客户端却不能从服务器端获得补丁。经过分析，Symantec 企业版是靠 NetBIOS 名称管理每台计算机的，而 Symantec 客户端也是靠 NetBIOS 名称“查找”并定位服务器地址的，解析 NetBIOS 名称需要“广播”，而 VLAN 是屏蔽广播的，所以 Symantec 服务器端不能管理其他 VLAN 中的工作站，而使用 WINS 就可以解决这个问题。

某单位有 5 台服务器，其中 1 台升级到 Windows Server 2003 的 Active Directory 网络，其余 4 台服务器加入到 Active Directory 并且使用“DFS（分布式文件系统）”作为“文件服务器”提供共享。但在使用中发现，虽然各个工作站都能访问 DFS 根目录，但 DFS 中的“链接”有的却不能打开，经过检查发现，凡是与服务器在同一 VLAN 的计算机都可以打开，凡是不在同一 VLAN 的计算机都不能打开。经过进一步检查，发现另外 4 台在提供 DFS 链接时，都是使用 NetBIOS 名称而不是 DNS 名称，因为网络中没有 WINS 服务器，所以其他 VLAN 中的计算机不能解析 NetBIOS 名称。知道问题所在后，就可以解决该问题了：第一种解决方法是将所有的 DFS 链接更换为 DNS 名称；第二种方法是在企业部署 WINS 服务器并用 WINS 服务器为所有计算机解析 NetBIOS 名称。

第 4 章　磁盘与文件系统管理

在操作系统中，尤其是对作为“服务器”的网络操作系统来说，合理并安全的管理存储资源是每个管理员需要承担的任务。在购买服务器的初期，每个管理员要为现在以及将来要用到的存储容量、存储性能及存储的安全性做出合理的规划。如果接手一个已经规划好的网络，怎样合理而安全的使用现有的服务器存储也是一个重要的任务。本章将介绍磁盘文件系统、NTFS 安全性、共享文件夹、BitLocker、磁盘配额、卷影副本等一系列与“存储”相关的内容。

4.1　磁盘与存储的关系

管理“存储”是操作系统的一项基本功能，这里所说的“存储”，既包括安装在计算机“本地的”磁盘所组成的“存储”，也包括通过网络连接的“网络存储”或专用连接线缆连接的“SAN 存储”等。

对于“本地磁盘”来说，在安装操作系统之前，就需要对其做出合理的规划。如果服务器具有支持 RAID5 或 RAID50、RAID6 的陈列卡，则需要先用陈列卡的配置程序，将服务器上的多个硬盘划分为 1 个或多个“逻辑磁盘”。在安装操作系统的时候，利用操作系统的安装程序，对其中的一个逻辑磁盘进行“分区”，并在其中的一个分区中安装操作系统。安装完操作系统之后，对剩余的空间或逻辑磁盘进行分区、格式化等工作，这样，本地的磁盘才能使用。在这里，采用 RAID 卡划分后的每个“逻辑磁盘”，相当于普通台式机中的“物理磁盘”，它们在逻辑上是等效的。或者这样理解：陈列卡运行于操作系统的更底层，经过陈列卡划分的每个磁盘，对于操作系统来说是单独的硬盘。

操作系统只能安装、运行于“本地磁盘”，或者相对于“操作系统”来说是“本地磁盘”。例如，如果物理主机安装了 Hyper-V 或 VMware ESX Server，且 Hyper-V 或 VMware ESX Server 使用了 iSCSI 网络存储，创建虚拟机并在虚拟机中安装操作系统。如果 Hyper-V 或 VMware ESX Server 将虚拟机分配于 iSCSI 网络存储，则对于 Hyper-V 或 VMware ESX Server 来说，iSCSI 存储是“网络存储”，而对于由 Hyper-V 或 VMware ESX Server 管理的虚拟机来说，则是“本地磁盘”、“本地存储”。

对于“网络存储”来说，在安装好操作系统之后，可以通过网络或专门的连接线缆，连接到存储服务器，存储服务器提供的存储供操作系统使用和管理。

4.1.1　采用何种 RAID 与磁盘

对于服务器来说，如果服务器的硬盘在 3～5 块，则推荐采用 RAID5，这样可以达到较好的性能及较高的安全性。如果服务器的硬盘在 6 块以上并且是偶数硬盘，则推荐采用 RAID50，这样可以实现更高的安全性。

现在服务器的磁盘普遍采用 SAS 接口，这种接口也兼容 SATA 接口，对于要求不是特别高的企业来说，推荐采用 SATA 硬盘，因为 SATA 硬盘具有最高的性价比。例如，一块 3.5 英寸、SAS 接口、600GB、15000 转的硬盘市场价大约在 3000 元以上，而一块 1TB、SATA 接口、7200 转的 3.5 英寸企业级硬盘，市场价大约是 800 元。为了达到较好的性能，可以用多块 SATA 硬盘来弥补磁盘转速的不足，并且，目前 SATA 硬盘可以做到单碟 500GB 甚至 1TB，较高的磁盘容量可以近一步降低转速所带来的问题。对于 SAS 与 SATA 硬盘来说，其内部数据传输率是比较接近的，在日常的使用中，对于大多数企业用户而言，差距不大。

4.1.2　关于服务器使用 RAID5 磁盘陈列的问题

一些服务器在创建磁盘陈列时，大多是把服务器上所有的硬盘创建 RAID5，并且只划分了一个“逻辑磁盘”，这样从理论上来讲没有任何问题，在实际中也是可以使用的，但是这种方法并不可取，原因在于：现在服务器集成的 SCSI、RAID 卡、SAS 卡等，操作系统大多没有集成相关的驱动程序，这样在安装操作系统的时候，如果使用 Windows Server 2003（或 Windows Server 2008）安装光盘，从光盘启动安装，在安装的时候需要按 F6，并在软驱中插入相关的 SCSI、RAID 卡驱动程序。而现在一些服务器并不带软驱（或者虽然服务器带软驱，但软盘质量太差了）。这个时候，就需要使用服务器带的“引导光盘”启动，使用服务器的引导光盘来安装系统，而采用这种方法的时候，要把第 1 个逻辑磁盘重新划分分区，这样做在第 1 次安装系统的时候没有问题，但如果服务器使用一段时间之后需要重新安装系统，并且 D 分区、E 分区有数据的时候，如果还用这种方法就不太现实了。

所以，上面这种方法，只是“能用”并不“实用”。推荐大家使用下面的方式划分：在创建 RAID5 或 RAID50 的磁盘陈列时，创建两个逻辑磁盘，第 1 个逻辑磁盘大小为 30～100GB，第 2 个逻辑磁盘是 RAID5 的剩余空间。这样，既使是使用服务器带的“引导光盘”安装系统，也只是把第 1 个逻辑磁盘重新划分分区，并不会影响第 2 个逻辑磁盘上的数据。另外，在使用服务器带的光盘划分第 1 个逻辑磁盘时，就把所有的空间都划分出来，这样第 1 个逻辑磁盘只安装系统，不做他用。

现在服务器大多安装了 4～6 个硬盘，这些硬盘可以创建 RAID5。如果服务器上有 10 个硬盘，不建议把这 10 个硬盘创建一个 RAID5，而应该是每 5 个硬盘一组，分别创建 RAID5。并且，第一组的 5 个硬盘，创建两个逻辑磁盘（第 1 个 30～100GB，第 2 个是 RAID5 的剩余空间），而第二组的 5 个硬盘，只需要创建一个逻辑磁盘专门存数据就行了。如果需要单一的大硬盘分区，只需要使用 Windows Server 2003、Windows Server 2008、Windows Server 2008 R2 中的“动态卷”，将第 2 个逻辑磁盘创建一个分区并附加到第一组第 2 个逻辑磁盘创建的分区就可以了。

最后还要告诉大家一点，就是在创建磁盘陈列时，没有备用的硬盘，而把所有的硬盘都使用上也是不可取的。通常情况下，陈列中的硬盘，大多在 3～5 年之后才开始出故障，如果这时 RAID5

中的 1 个硬盘出现问题，需要将故障硬盘替换下来，但是在 3 年之后很少能买到 3 年甚至更长时间以前的硬盘。另外，数据也没有时间等待购买硬盘。所以，在做磁盘陈列的时候，甚至在前期规划的时候，相同的硬盘至少得有一、两块备用的，当服务器硬盘有故障时马上替换，而不是关闭服务器、向领导打报告、等领导指示后再买硬盘替换。

综上所述，如果使用磁盘陈列，尤其是提供虚拟化应用的服务器，一定要有备用硬盘，并且按照上述所介绍的方式划分分区，这样可以减少出现问题的概率，做到防患于未然。

4.2　文件系统概述

文件系统是计算机用于组织硬盘上的数据的基本结构。如果要安装新硬盘，则需要使用文件系统对其进行分区和格式化，然后才能开始存储数据或程序。Windows 中，可以从中进行选择的三个文件系统选项为：NTFS、FAT32 以及现在很少使用的较早的 FAT（也称 FAT16）。

4.2.1　NTFS

NTFS 是 Windows 版本（Windows Server 2008 R2）的首选文件系统。与早期的 FAT32 文件系统相比，它有许多优点，其中包括：

- 能够从某些与磁盘相关的错误中自动恢复，而 FAT32 则不能。
- 改善了对较大硬盘的支持。
- 由于可以使用权限和加密来限制用户访问特定文件，因此安全性更好。

如果要将 FAT32 文件系统转换为 NTFS 文件系统，可以进入“命令提示窗口”，执行 convert 命令，并加上相关的参数，将指定的磁盘转换为 NTFS 文件系统。例如，如果要将 D 分区转换为 NTFS 文件系统，可以执行如下的命令：

```
convert d:   /fs:ntfs
```

在执行该命令之后，根据屏幕的提示进行操作既可。

4.2.2　FAT32

FAT32 以及更少使用的 FAT 用于早期版本的 Windows 操作系统，包括 Windows 95、Windows 98 和 Windows Millennium Edition。FAT32 不具有 NTFS 提供的安全性， 因此如果计算机上有 FAT32 分区或卷，则访问该计算机的任何用户都可以读取上面的文件。FAT32 还有大小限制，不能在此 Windows 版本中创建大于 32GB 的 FAT32 分区，也不能在 FAT32 分区上存储大于 4GB 的文件。

使用 FAT32 的主要原因是计算机有时既需要运行 Windows 95、Windows 98 或 Windows Millennium Edition，又需要运行此 Windows 版本，这称为多重引导配置。如果是这种情况，则需要在 FAT32 或 FAT 分区上安装早期版本的操作系统并确保它是主分区（可以驻留操作系统的分区）。使用这些早期的 Windows 版本时，需要访问的其他任何分区都必须使用 FAT32 格式化。

这些早期的 Windows 版本可以访问网络上的 NTFS 分区或卷，但不能访问计算机上的 NTFS 分区或卷。

4.3 磁盘与卷管理

基本磁盘和动态磁盘是 Windows 中的两种硬盘配置类型。大多数个人计算机都配置为基本磁盘，该类型易于管理。而动态磁盘可以使用计算机内的多个硬盘复制数据，从而提高了性能和可靠性。

基本磁盘使用主分区、扩展分区和逻辑驱动器组织数据。格式化的分区也称为卷（术语“卷”和“分区”通常互换使用）。在此 Windows 版本中，基本磁盘可以有四个主分区或三个主分区和一个扩展分区。扩展分区可以包含无数个逻辑驱动器。基本磁盘上的分区不能与其他分区共享或拆分数据。基本磁盘上的每个分区都是该磁盘上一个独立的实体。

动态磁盘可以包含无数个“动态卷”，其功能与基本磁盘上主分区的功能相似。基本磁盘和动态磁盘之间的主要区别在于动态磁盘可以在计算机上的两个或多个动态硬盘之间拆分或共享数据。例如，一个动态卷实际上可以由两个单独的硬盘上的存储空间组成。另外，动态磁盘可以在两个或多个硬盘之间复制数据以防止单个磁盘出现故障。此功能需要更多硬盘，但提高了可靠性。

在下面的操作中，我们将向实验用的 Windows Server 2008 R2 虚拟机中添加两块新的虚拟硬盘，用于动态卷的实验。

4.3.1 添加虚拟硬盘

关闭 Windows Server 2008 R2 虚拟机，向虚拟机中添加两块虚拟硬盘用于实验，主要步骤如下。

01 在 Hyper-V 控制台中，确认 Windows 2008 R2 虚拟机处于关闭状态，然后用鼠标右键单击，在弹出的快捷菜单中选择“设置”按钮，如图 4-1 所示。

02 在虚拟机设置中，在“IDE 控制器 0”中单击“添加”按钮，如图 4-2 所示。

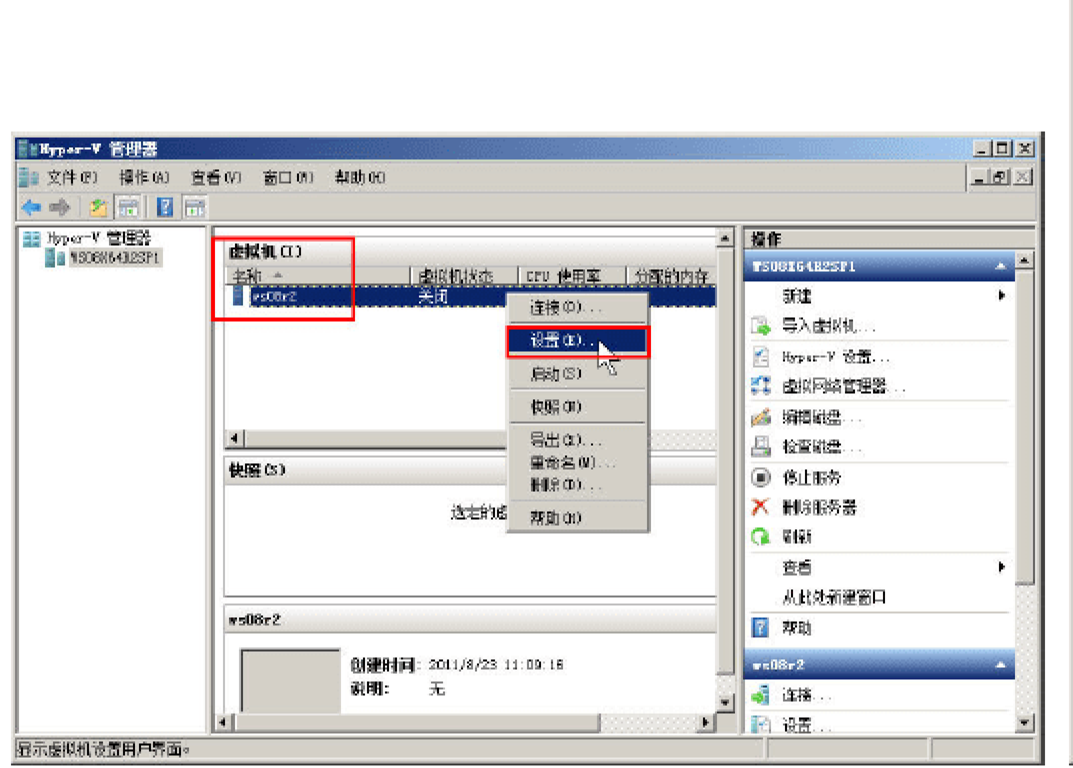


图 4-1　设置

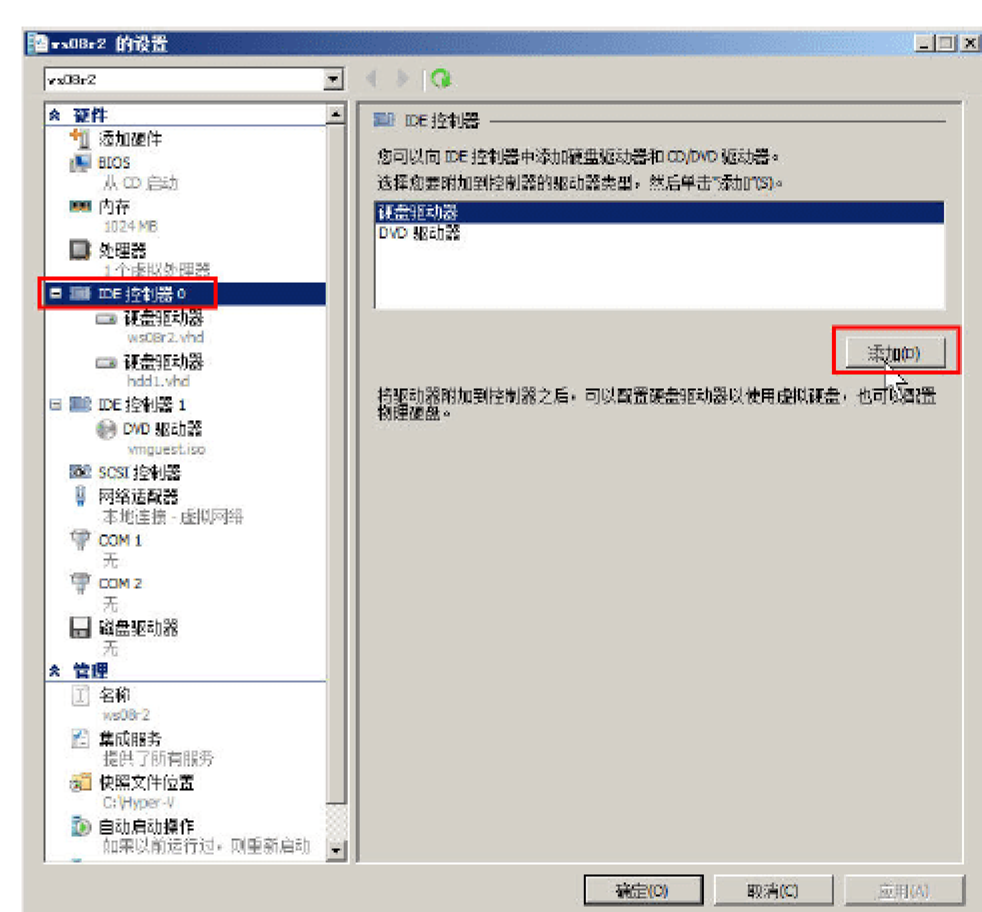


图 4-2　添加

03 在“硬盘驱动器”窗口中，单击“新建”按钮，如图 4-3 所示。

04 在“开始之前”对话框中，选中“不再显示此页”复选框，如图 4-4 所示。

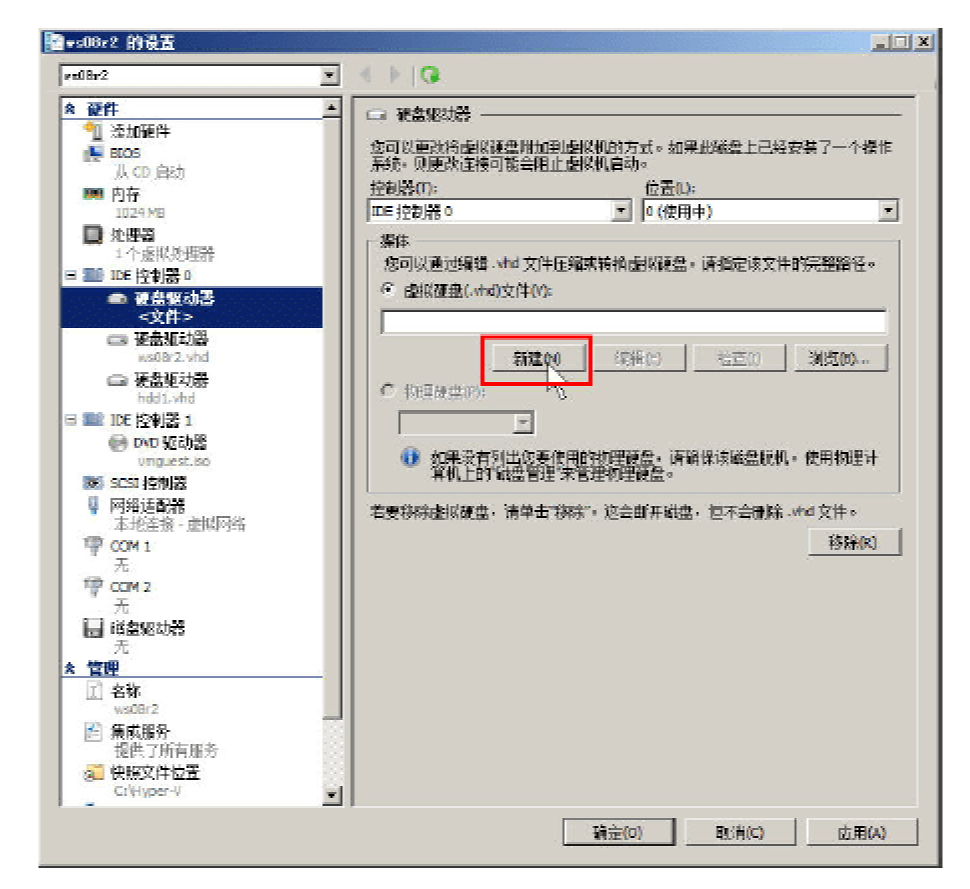


图 4-3　新建虚拟磁盘

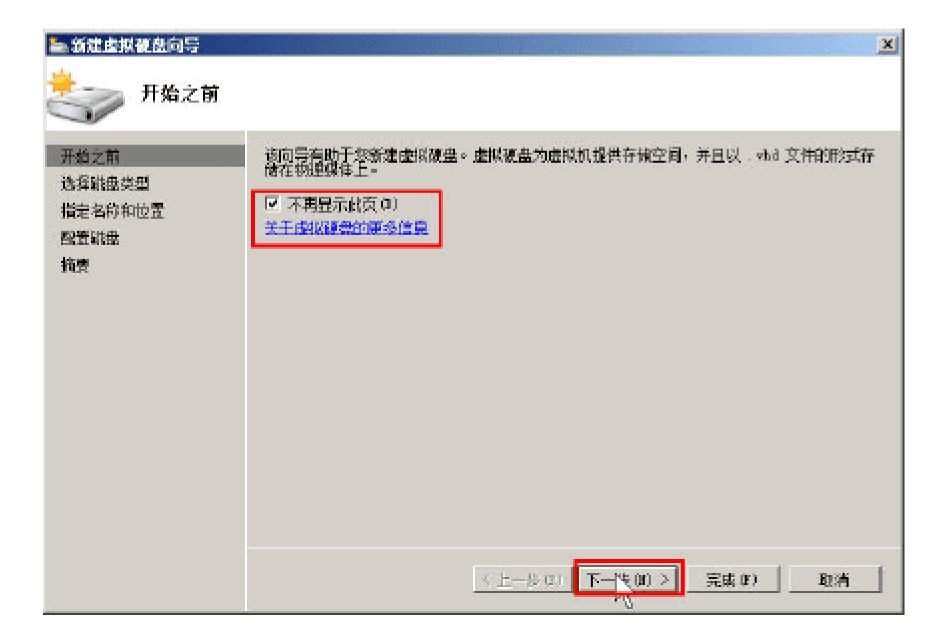


图 4-4　不再显示向导页

05 在“选择磁盘类型”对话框中，选中“动态扩展”单选按钮，创建一个动态扩展的虚拟磁盘，如图 4-5 所示。

06 在“指定名称和位置”对话框中，指定虚拟硬盘文件的名称和位置，如图 4-6 所示。



图 4-5　创建动态扩展磁盘



图 4-6　指定磁盘文件的名称和位置

07 在“配置磁盘”对话框中，指定新创建的虚拟硬盘的大小，在此选择默认值 16384MB（既 16GB），如图 4-7 所示。

08 创建虚拟磁盘向导完成，单击“完成”按钮，如图 4-8 所示。

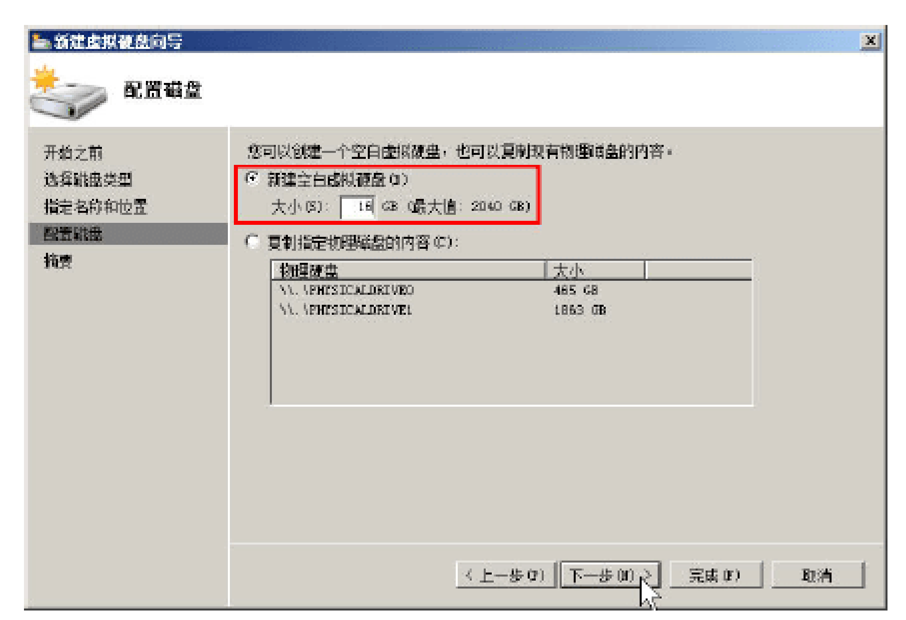


图 4-7　指定虚拟硬盘大小

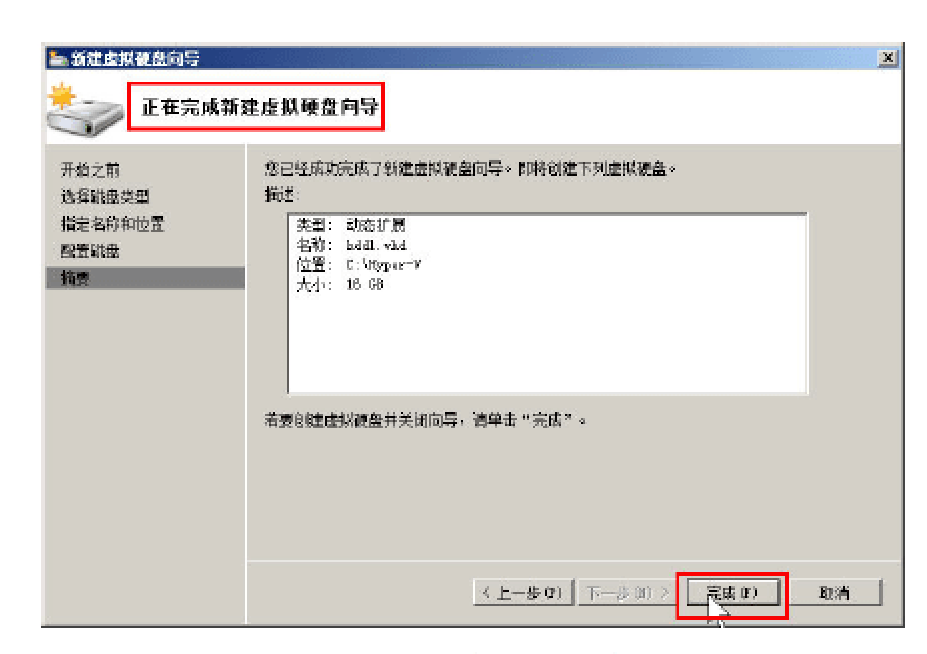


图 4-8　创建虚拟硬盘完成

09 返回到虚拟机设置对话框，确认新添加的磁盘（系统中第 2 个磁盘）“控制器”为“IDE 控制器 0”，“位置”为“1（使用中）”，如图 4-9 所示。

10 参照步骤 2~9，再次添加一个虚拟磁盘，使用“IDE 控制器 1”，“位置 1”，如图 4-10 所示。选择之后，单击“确定”按钮，完成设置。

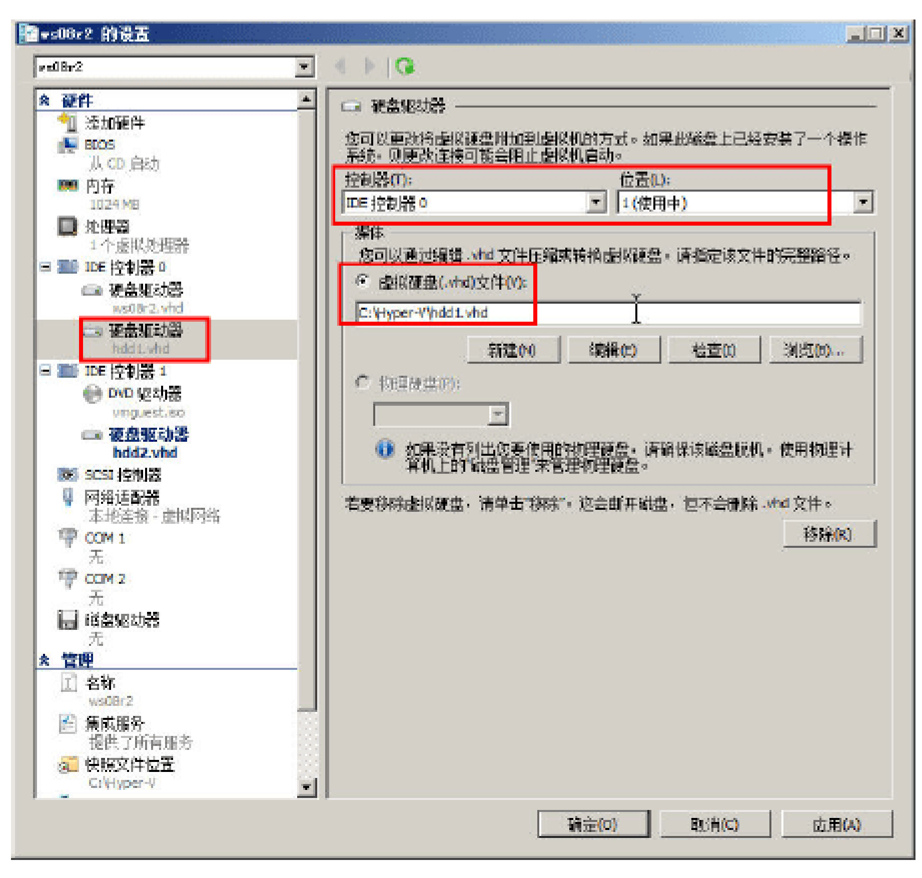




图 4-9　添加第 2 块硬盘

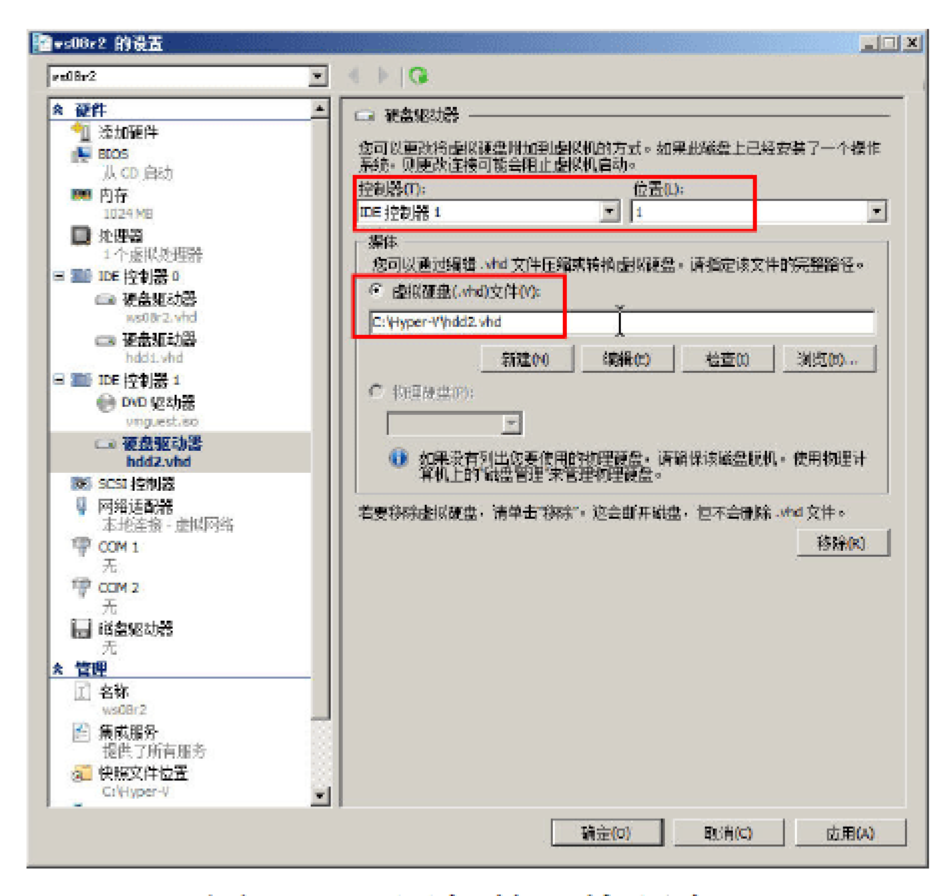


图 4-10　添加第 3 块硬盘

设置完成之后，在 Hyper-V 控制台，启动 Windows 2008 R2 虚拟机。

4.3.2　初始化新添加的硬盘

在做磁盘 RAID 的实验之前，操作系统会对新添加的硬盘进行初始化工作，具体如下所示。

01 启动 Windows 2008 虚拟机，进入系统后，选择“开始→所有程序→管理工具→计算机管理”进入“计算机管理”。

02 在打开的“计算机管理”对话框中，单击“存储→磁盘管理”项，因为新添加了硬盘，系统进入初始化磁盘向导，在“初始化磁盘”对话框中，选择将要初始化的硬盘，单击“确定”按钮，如图 4-11 所示。

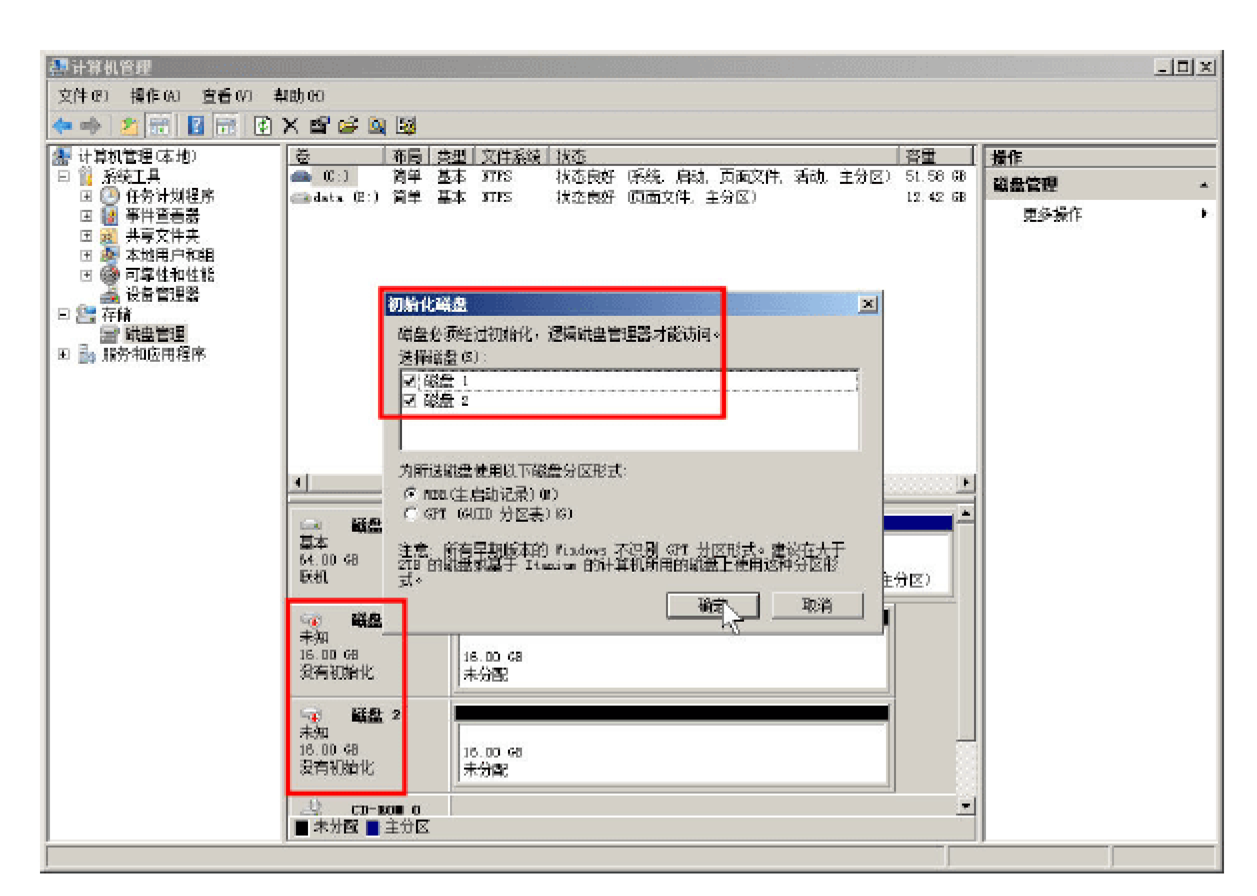


图 4-11　选择要初始化的磁盘



说 明

在图 4-11 中可以看到，没有初始化的磁盘其状态为“未知”。

初始化磁盘之后，既可以开始下面的学习。

4.3.3　创建镜像卷（RAID 1）

镜像卷（RAID1 功能）是在两个物理磁盘上复制数据的容错卷。通过使用两个相同的卷（被称为“镜像”），镜像卷（也叫 RAID1）提供了数据冗余，以便复制包含在卷上的信息。镜像总是位于另一个磁盘上。如果其中一个物理磁盘出现故障，则该故障磁盘上的数据将不可用，但是系统可以在位于其他磁盘上的镜像中继续进行操作（只能在运行 Windows 2000 Server 或 Windows Server 2003 、Windows Server 2008 操作系统的计算机的动态磁盘上创建镜像卷）。在本次实验中，将创建一个 RAID 1 的磁盘组，大小为 1024MB（既 1GB）。具体操作步骤如下所示。

01 在“磁盘管理”中，选择第 2 块硬盘，用鼠标右击硬盘，在弹出的菜单中选择“新建镜像卷”命令，如图 4-12 所示。

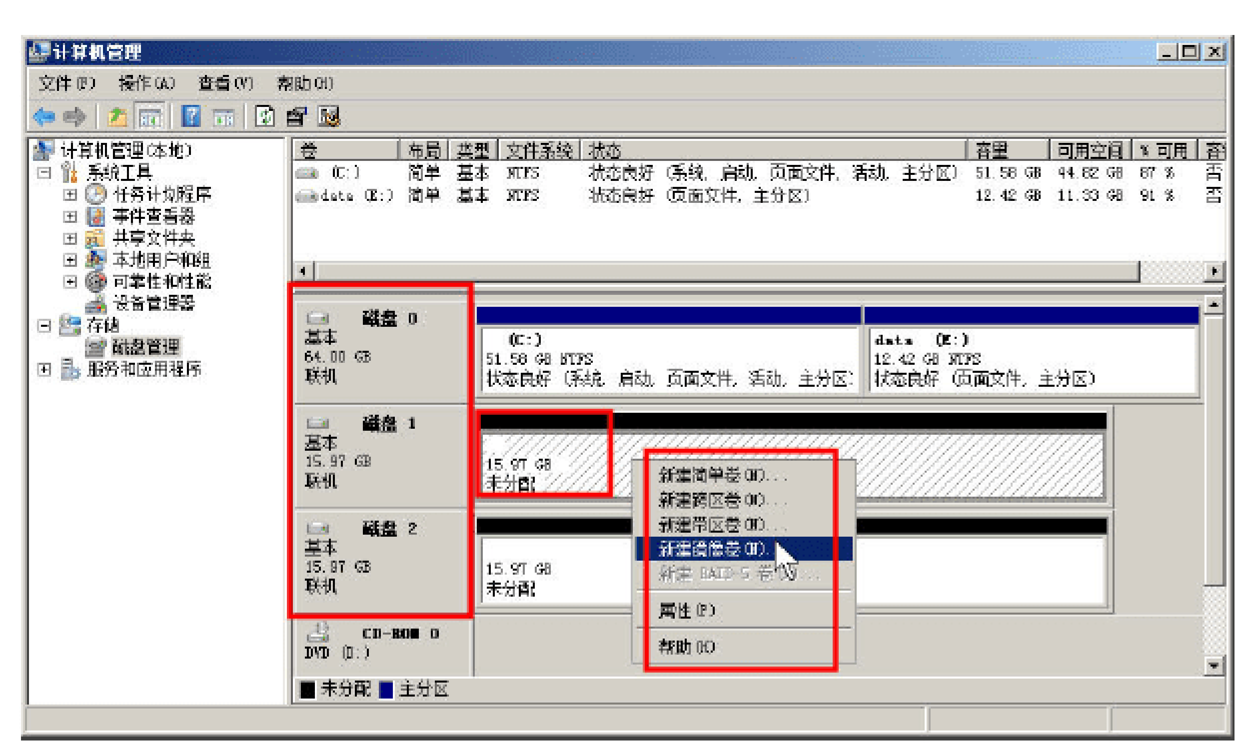


图 4-12　新建镜像卷



说 明

在图 4-12 中可以看到，当前系统中有 3 个硬盘，分别是磁盘 0（这是原来安装操作系统的硬盘）、磁盘 1 和磁盘 2。其中后两个磁盘是新添加的虚拟硬盘，大小约为 16GB。在图中也可以看到，磁盘 0、磁盘 1、磁盘 2 目前都属于“基本”磁盘。

02 在“欢迎使用新建镜像卷向导”对话框中，单击“下一步”按钮，进入新建卷向导，如图 4-13 所示。

03 在“选择磁盘”对话框中，在可用磁盘中选中磁盘 2，然后单击“添加”按钮，将其添加到“已选的”列表中，如图 4-14 所示。

04 添加完一块磁盘后，由于创建的是镜像卷不能再添加磁盘，在“选择空间量”文本框中设置镜像卷大小为 1024M，然后单击“下一步”按钮，如图 4-15 所示。

05 在“分配驱动器号和路径”对话框中，为新添加的卷指派盘符为 F，然后单击“下一步”按钮，如图 4-16 所示。

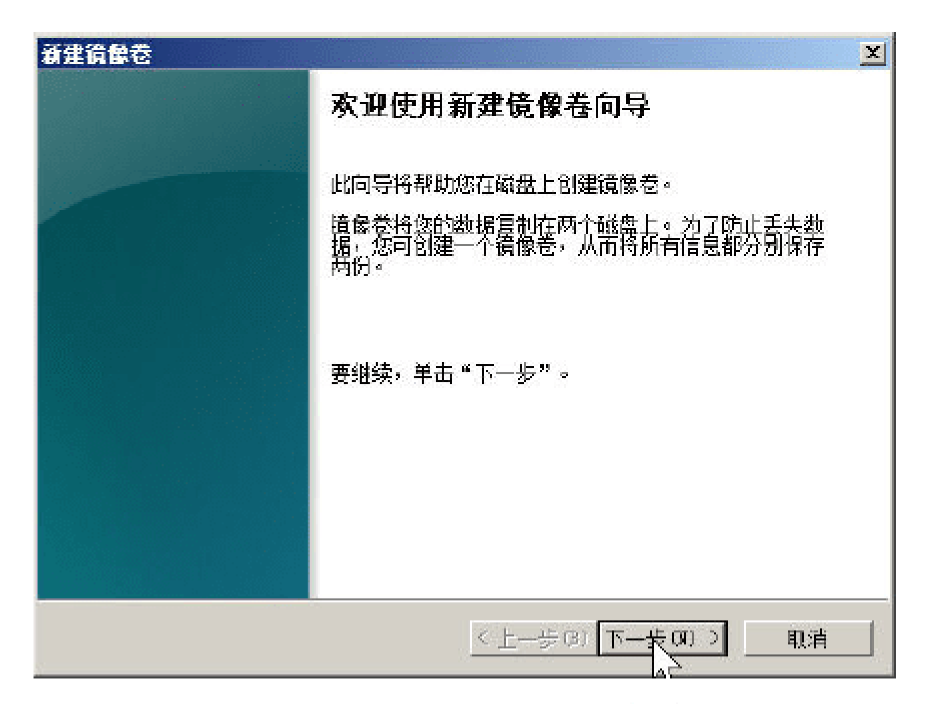


图 4-13　进入新建卷向导

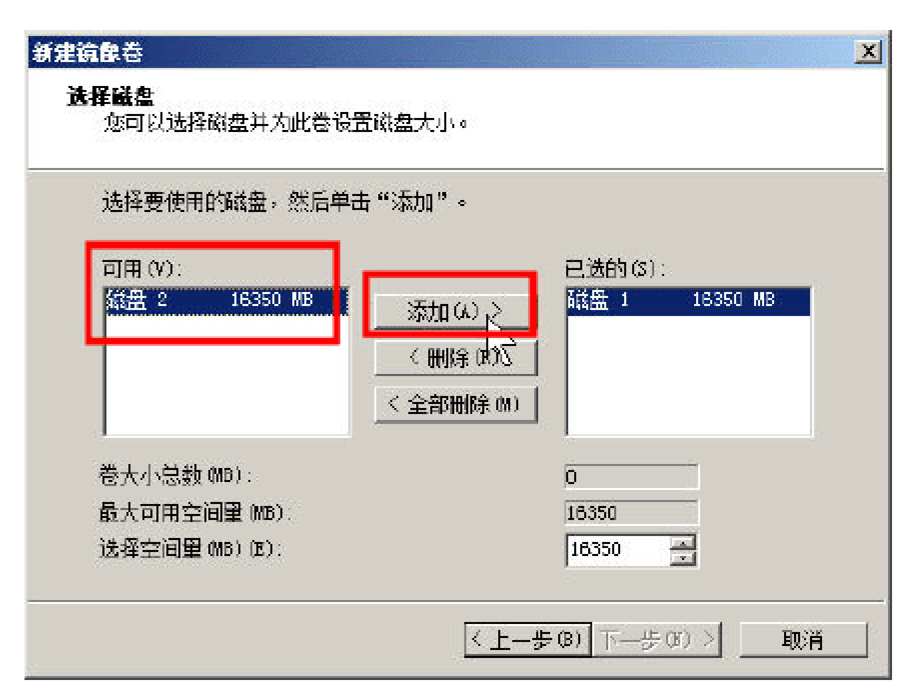


图 4-14　添加磁盘

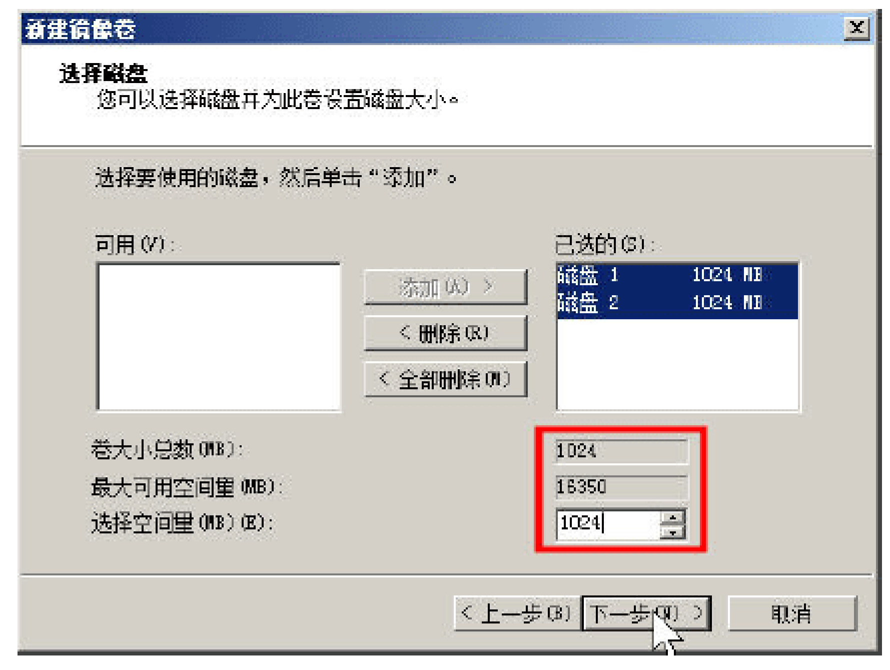


图 4-15　设置卷大小

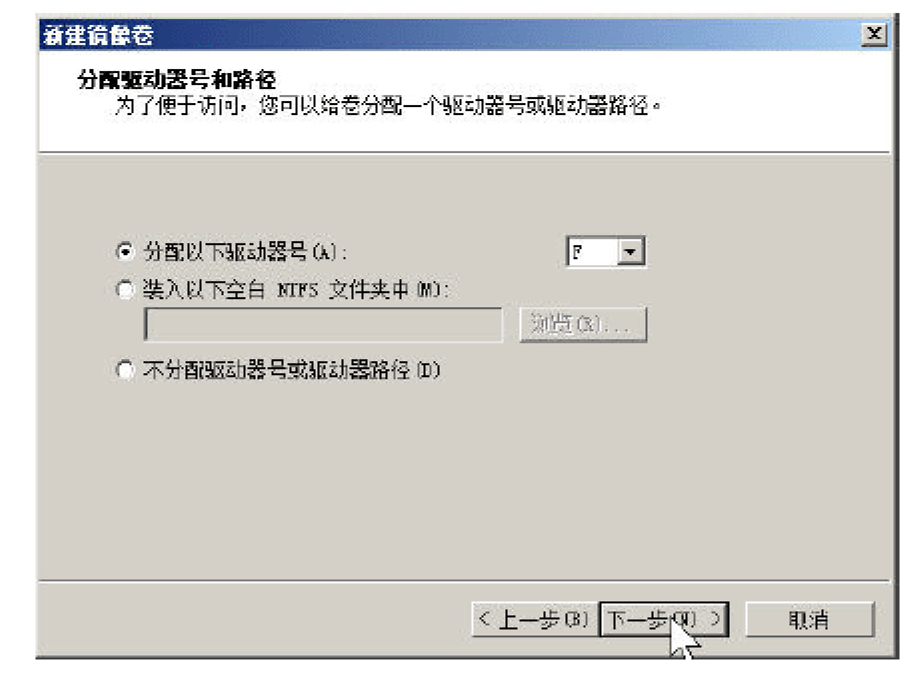


图 4-16　为新添加的卷指派驱动器号

06 在“卷区格式化”对话框中，设置卷标名为“RADI1”，并且选中“执行快速格式化”复选框，单击“下一步”按钮，如图 4-17 所示。

07 完成新建卷向导后，在“正在完成新建镜像卷向导”对话框中，单击“完成”按钮，如图 4-18 所示。

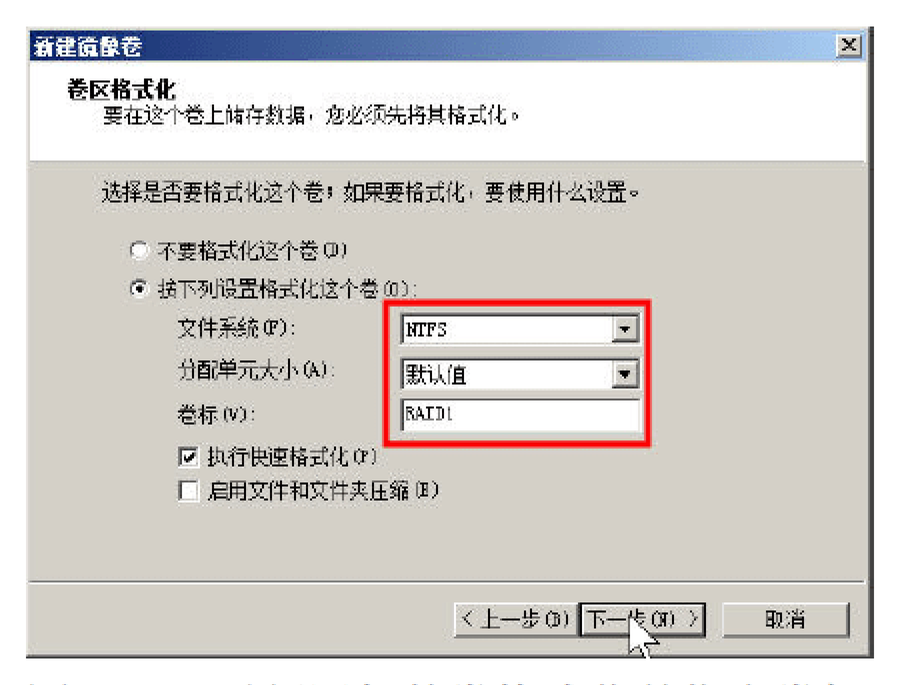


图 4-17　对新添加的卷格式化并指定卷标

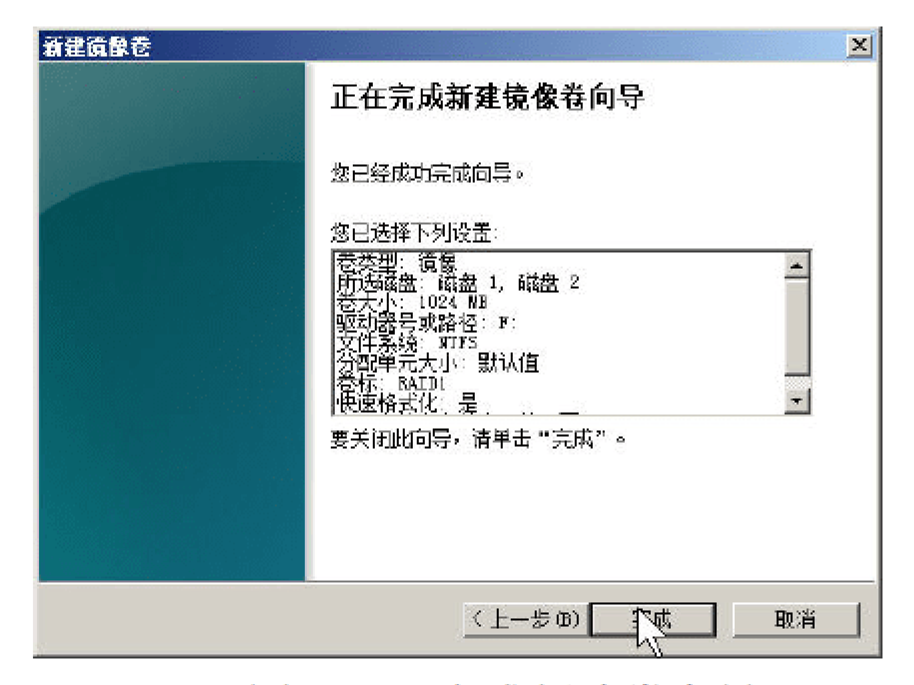


图 4-18　完成新建卷向导

08 在弹出的“磁盘管理”提示框中，系统提示要将“基本磁盘”转换为“动态磁盘”，单击“是”按钮进行转换，如图 4-19 所示。

09 在“磁盘管理”对话框可以看到已经创建的镜像卷，并且磁盘 1、磁盘 2 已经转换成“动态”磁盘，如图 4-20 所示。

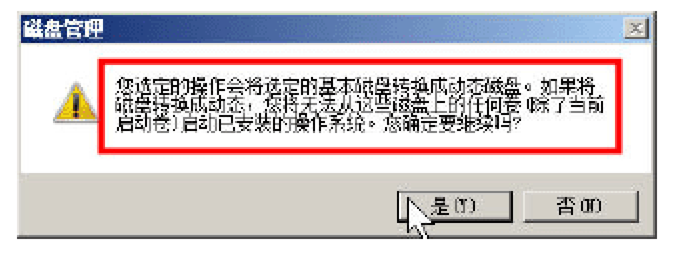


图 4-19 转换为动态磁盘

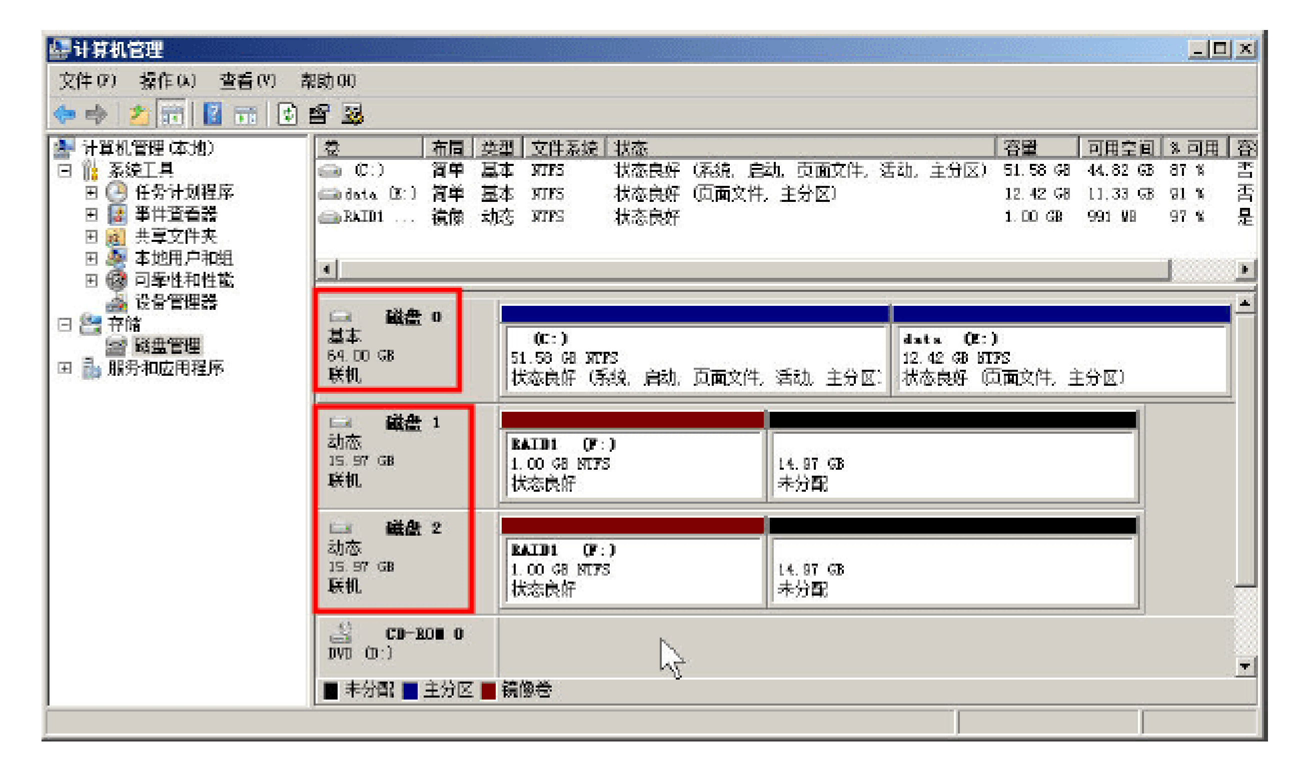


图 4-20 格式化新建卷

10 创建镜像卷完成后，用“褐色”表示。

4.3.4 创建 RAID 5 卷

在 Windows Server 2003、Windows Server 2008 中，RAID 5 卷是带有数据和奇偶校验带区的容错卷，间歇分布于三个或更多物理磁盘。奇偶校验是用于在发生故障后重建数据的计算值。如果物理磁盘的某一部分发生故障，Windows 会从其余的数据和奇偶校验重新创建发生故障的那部分磁盘上的数据（只能在运行 Windows 2000 Server 或 Windows Server 2003、Windows Server 2008 操作系统的计算机的动态磁盘上创建 RAID 5 卷）。无法镜像或扩展 RAID 5 卷。接下来我们将创建一个 RAID 5 的磁盘组，大小为 2GB。

由于 RAID5 卷需要至少 3 个磁盘，所以，我们将会把“磁盘 0”的 E 分区删除，并将其转换为动态磁盘。由于在以后的操作中，将 E 也设置为“页面交换”文件，在操作之前，需要先删除 E 分区上的“页面文件”，其主要步骤如下。

01 打开“虚拟内存”对话框，设置 E 分区上“无分页文件”，如图 4-21 所示。设置之后，先不要重新启动计算机。

02 返回到“计算机管理→磁盘管理”，右击“磁盘 0”，在弹出的快捷菜单中选择“转换成动态磁盘”，如图 4-22 所示。

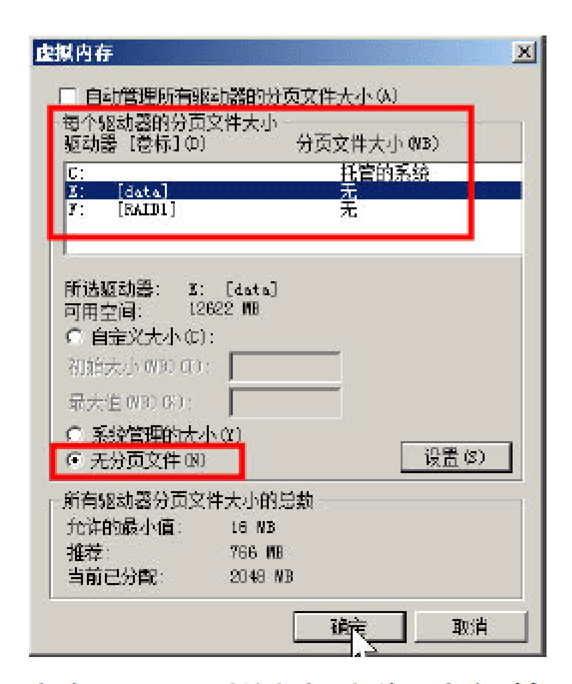


图 4-21 设置无分页文件

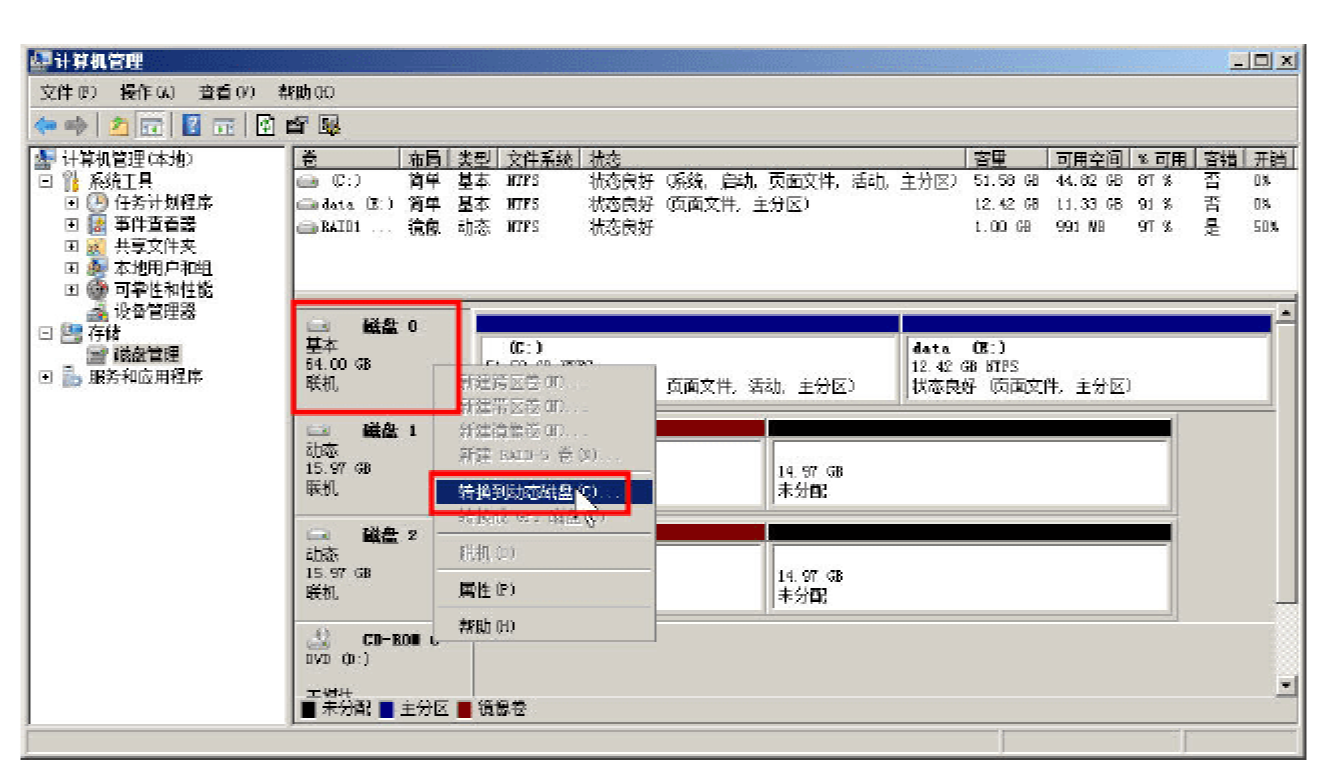


图 4-22 转换成动态磁盘

03 转换成动态磁盘之后，重新启动计算机。

04 再次进入系统后，打开“计算机管理→磁盘管理”，删除 E 分区，如图 4-23 所示。

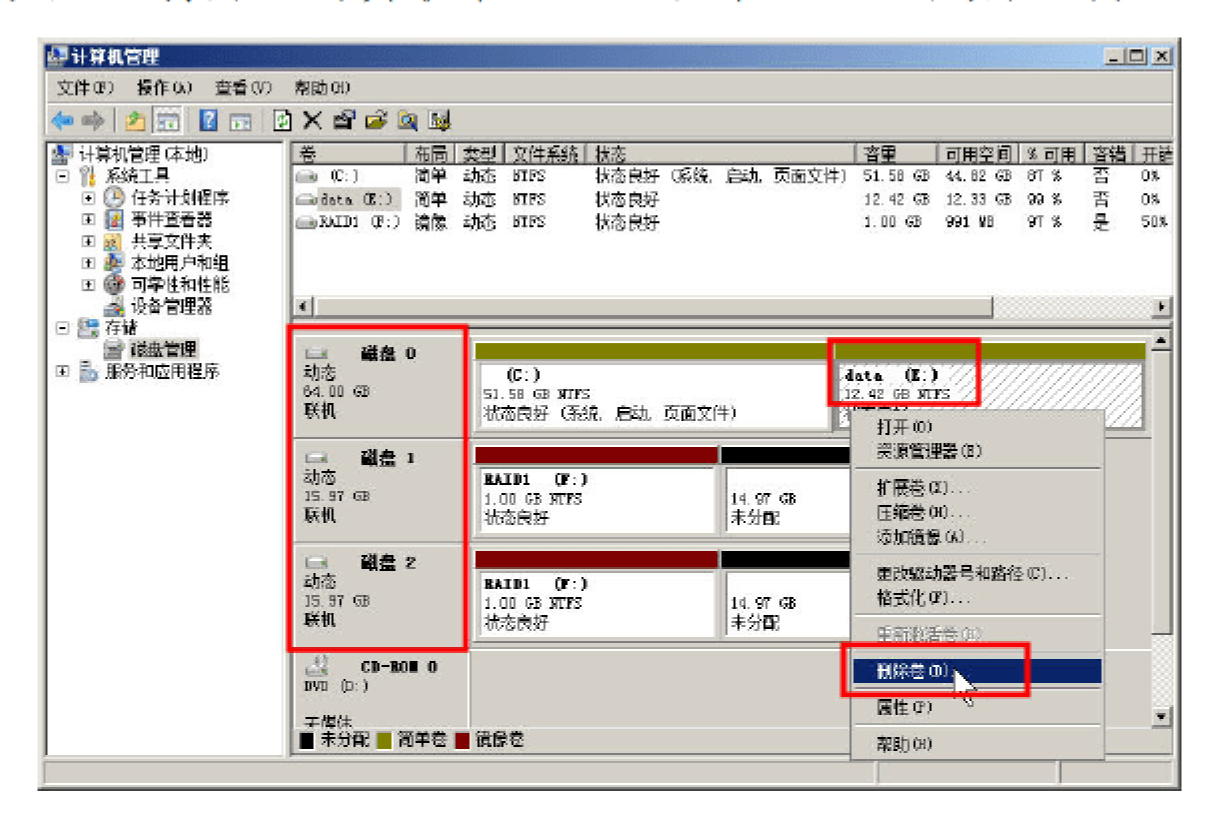


图 4-23　删除 E 分区

然后创建 RAID5 卷，步骤如下。

01 在“磁盘管理”窗格，选中“磁盘 0”空余空间，用鼠标右击，在弹出的菜单中选择“新建 RAID-5 卷”命令，如图 4-24 所示。

02 在“选择磁盘”对话框中，添加磁盘 1、磁盘 2 两块硬盘，在“选择空间量”处选择 1024，这样表示每个磁盘使用 1024MB，则 RAID5 可用空间为 2048MB，如图 4-25 所示。

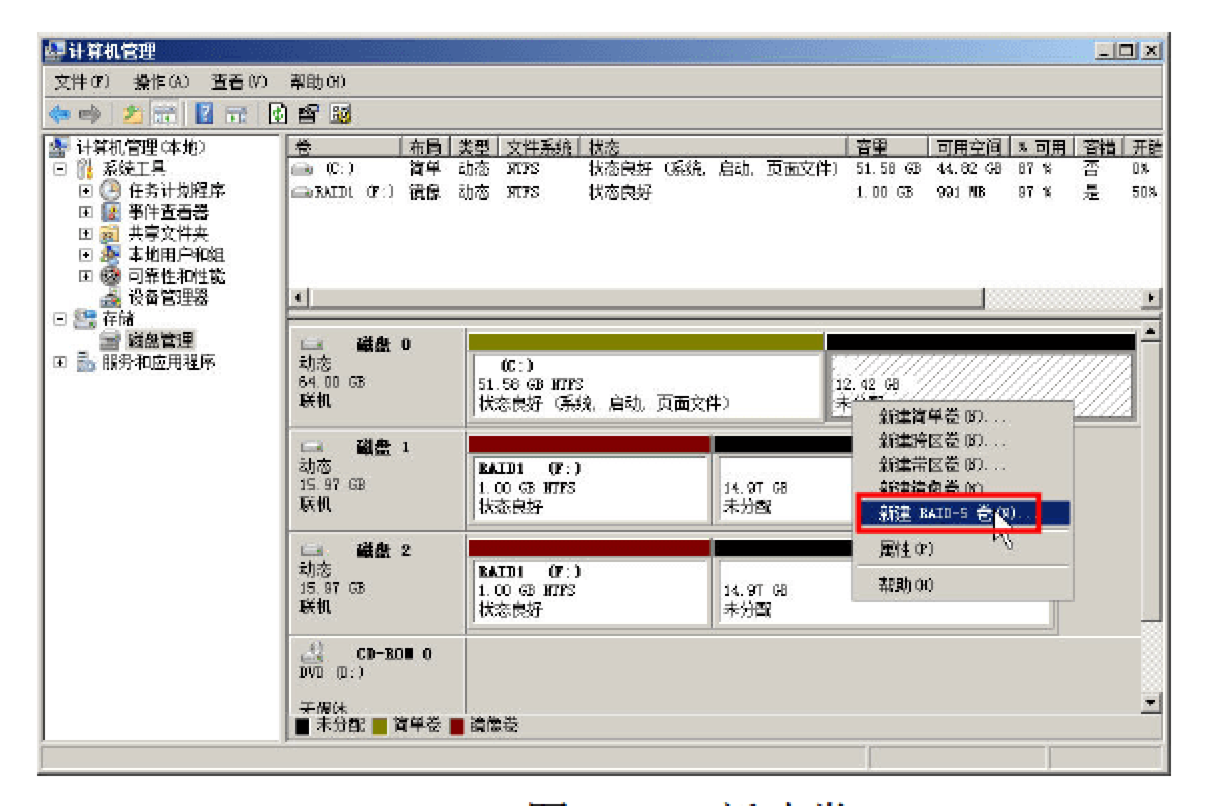


图 4-24　新建卷

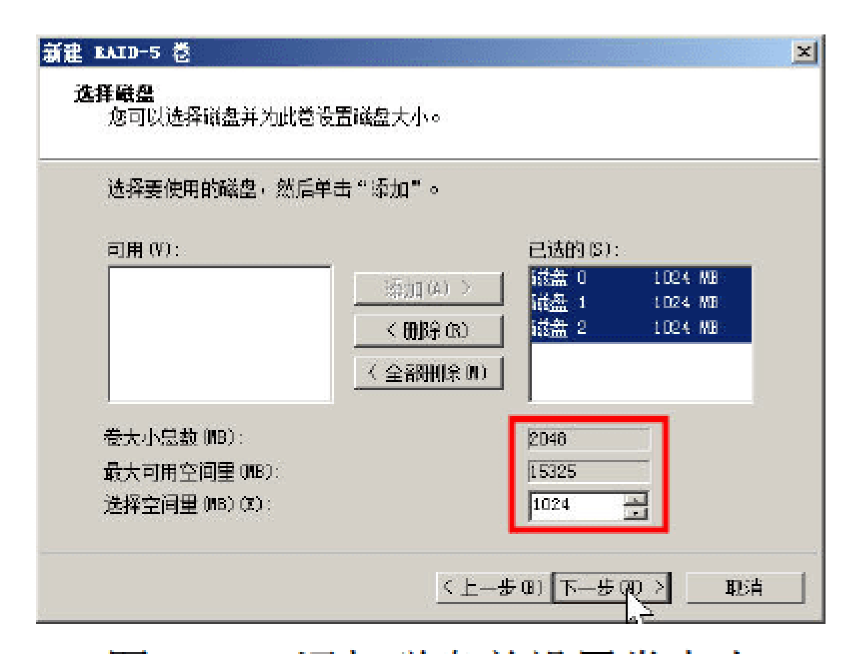


图 4-25　添加磁盘并设置卷大小

03 在“分配驱动器号和路径”对话框中，为新建的卷分配盘符为 E，如图 4-26 所示。

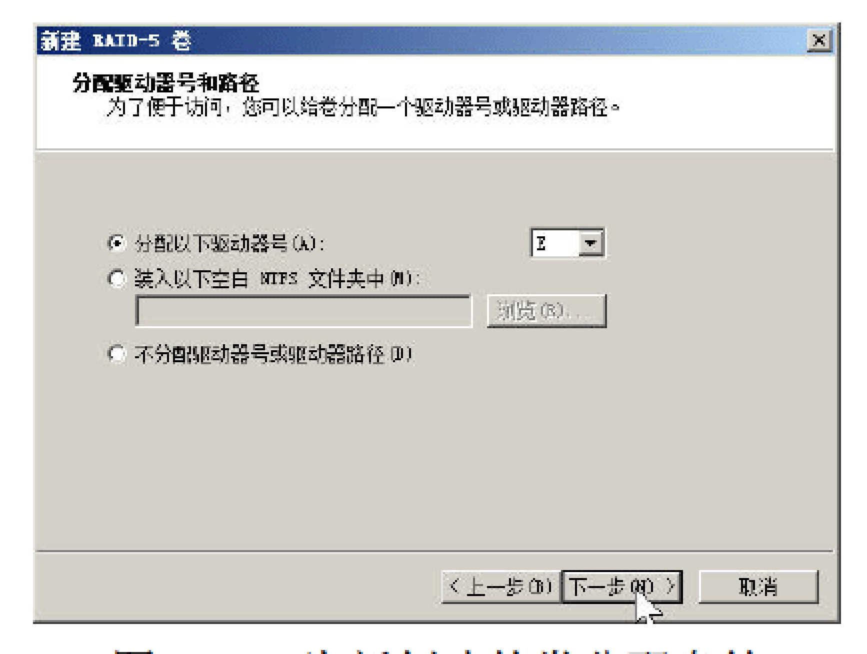


图 4-26　为新创建的卷分配盘符

04 在“卷区格式化”对话框中，设置卷标名为“RAID5”，并选中“执行快速格式化”复选框，然后单击“下一步”按钮，如图 4-27 所示。

05 RAID5 卷创建完成后，用“青绿色”表示，如图 4-28 所示。

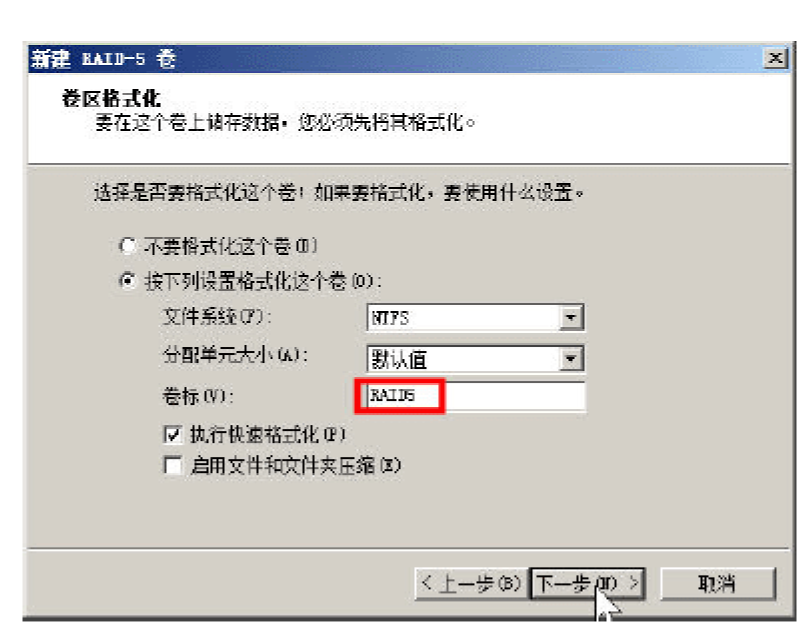


图 4-27　格式化新建卷并设置卷标

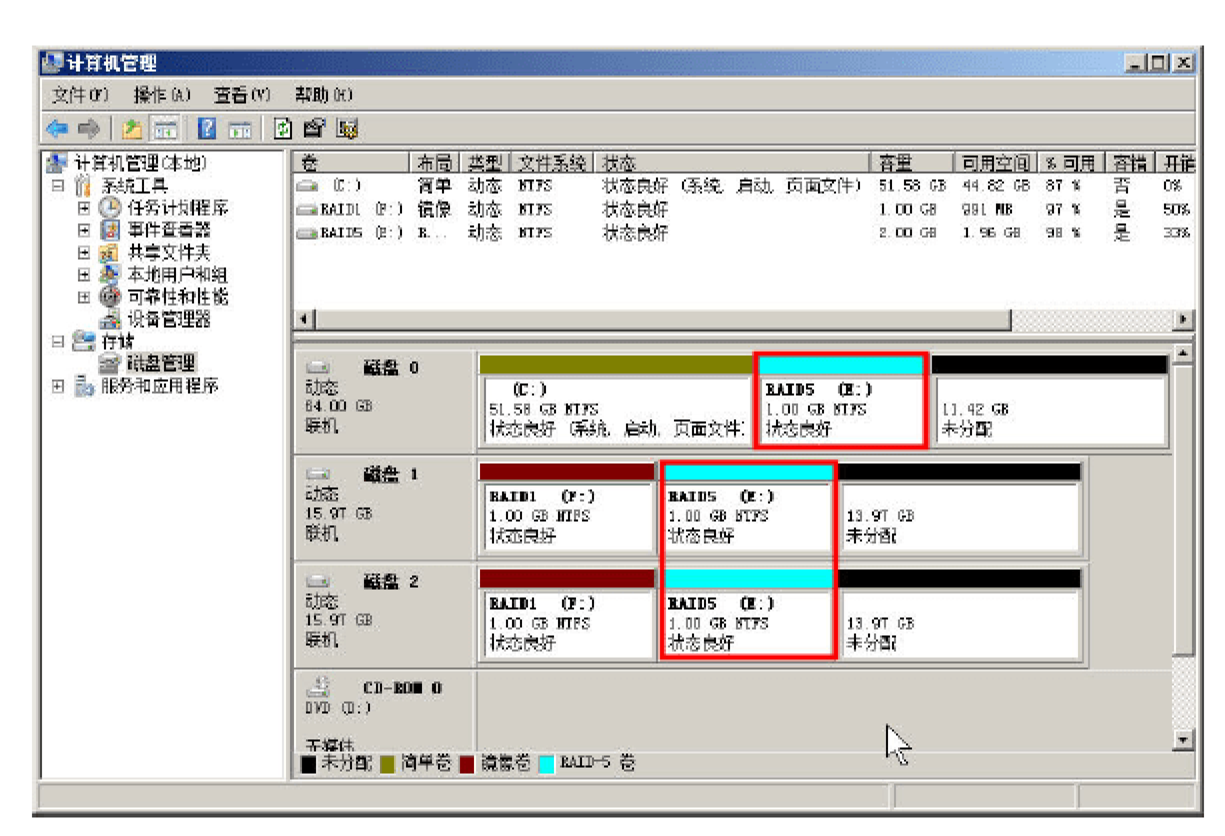


图 4-28　创建 RAID5 卷完成

4.3.5　带区卷实验（RAID 0）

带区卷是以带区形式在两个或多个物理磁盘上存储数据的卷，是 Windows 的所有可用卷中性能最佳的卷，但它不提供容错。带区卷上的数据被交替、均匀（以带区形式）地跨磁盘分配。如果带区卷中的磁盘发生故障，则整个卷中的数据都将丢失。只能在动态磁盘上创建带区卷，带区卷不能被镜像或扩展。Windows Server 2008 中的“带区卷”相当于 RAID 0。本次实验将使用 3 块硬盘、每个磁盘使用 1024MB 创建“带区卷”，创建之后，该卷空间为 1024MB×3=3076MB。操作步骤如下所示。

01 在“磁盘管理”窗格中，选中其中 1 块磁盘的剩余空间，用鼠标右击，在弹出的菜单中选择“新建带区卷”命令，如图 4-29 所示。

02 在“选择磁盘”对话框中，添加另外 2 块硬盘，并指定跨区卷硬盘空间大小为 1024MB，如图 4-30 所示。

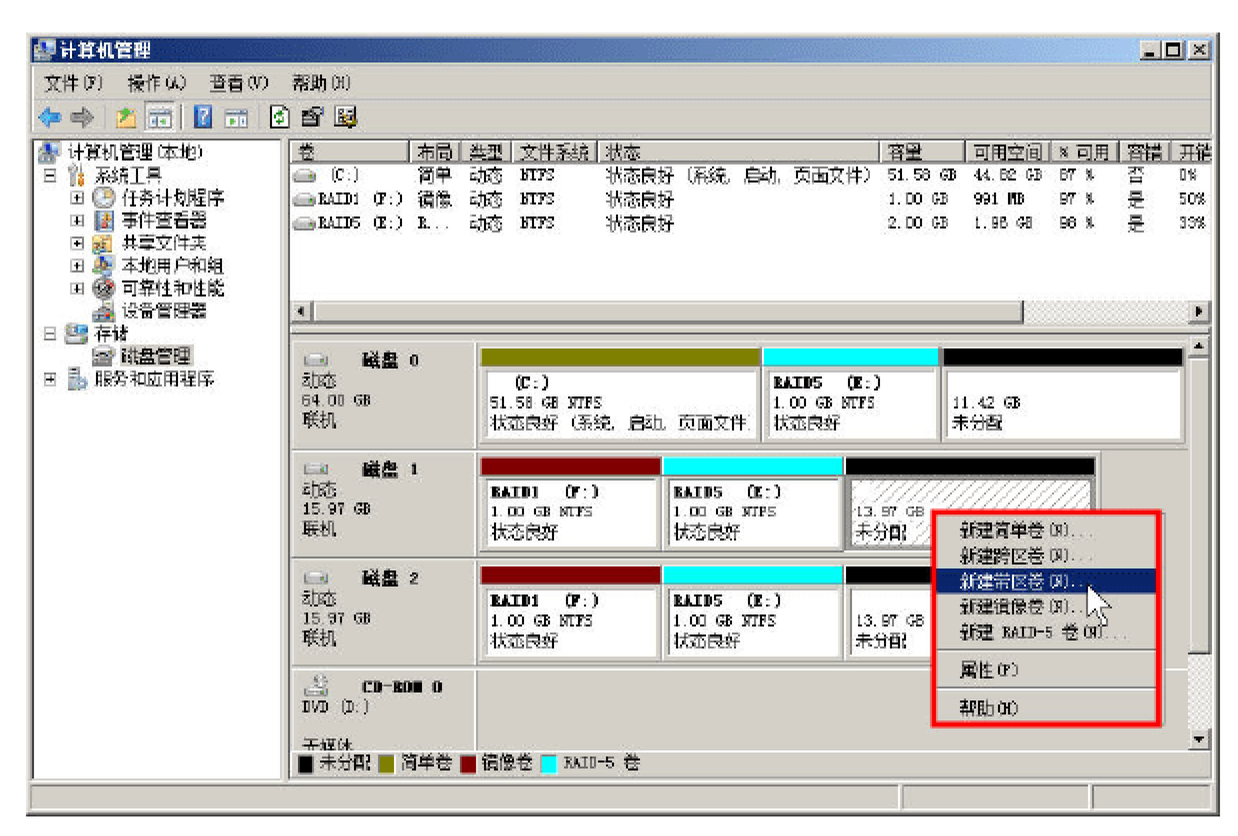


图 4-29　新建带区卷

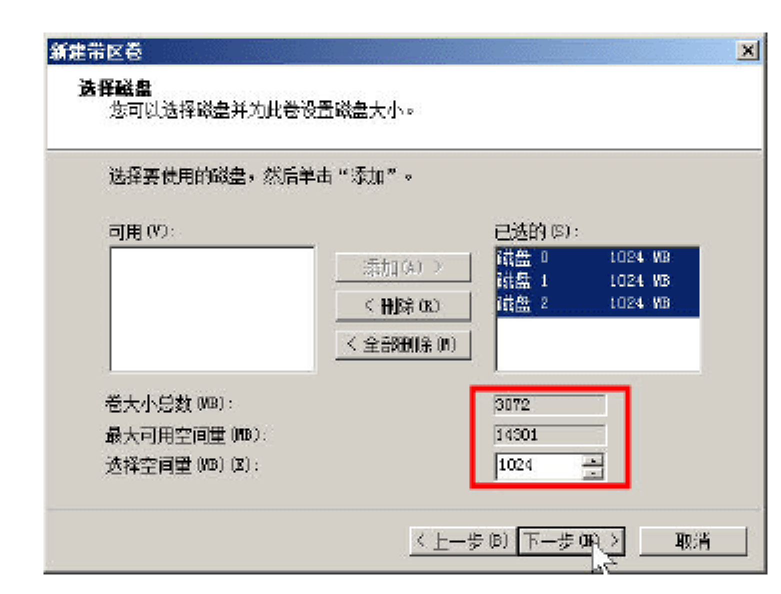


图 4-30　为带区卷添加硬盘并分配空间

03 在“分配驱动器号和路径”对话框中，为带区卷指定盘符为 G，如图 4-31 所示。

04 在“卷区格式化”对话框中，设置卷标为“RAID0”并且选中“执行快速格式化”复选框，如图 4-32 所示。

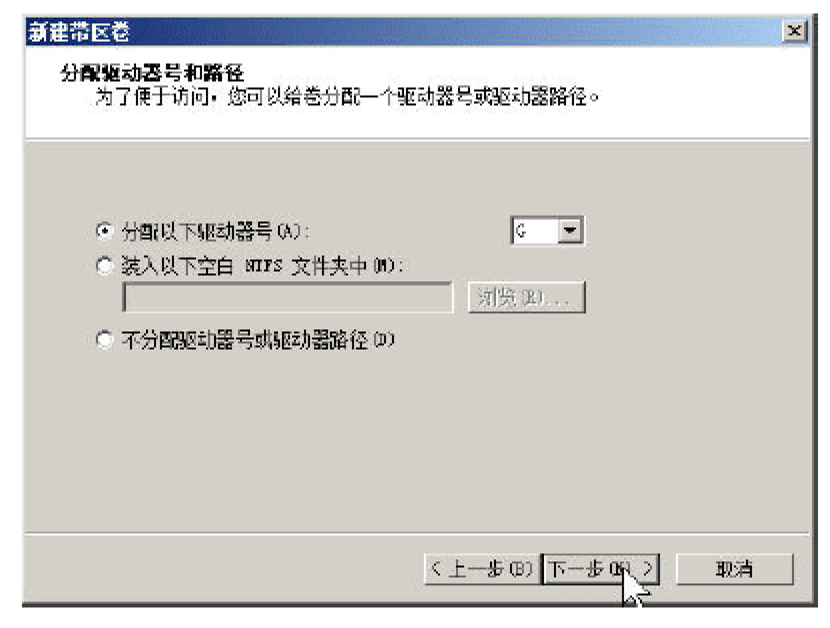


图 4-31　为新建卷分配盘符

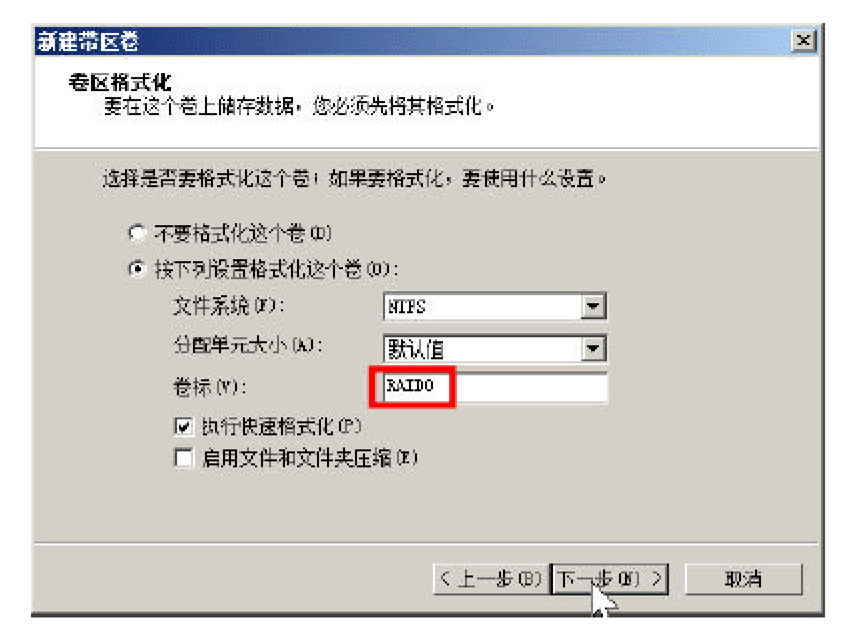


图 4-32　格式化新建卷并设置卷标

05 创建完成后，带区卷用“海绿色”表示，如图 4-33 所示。

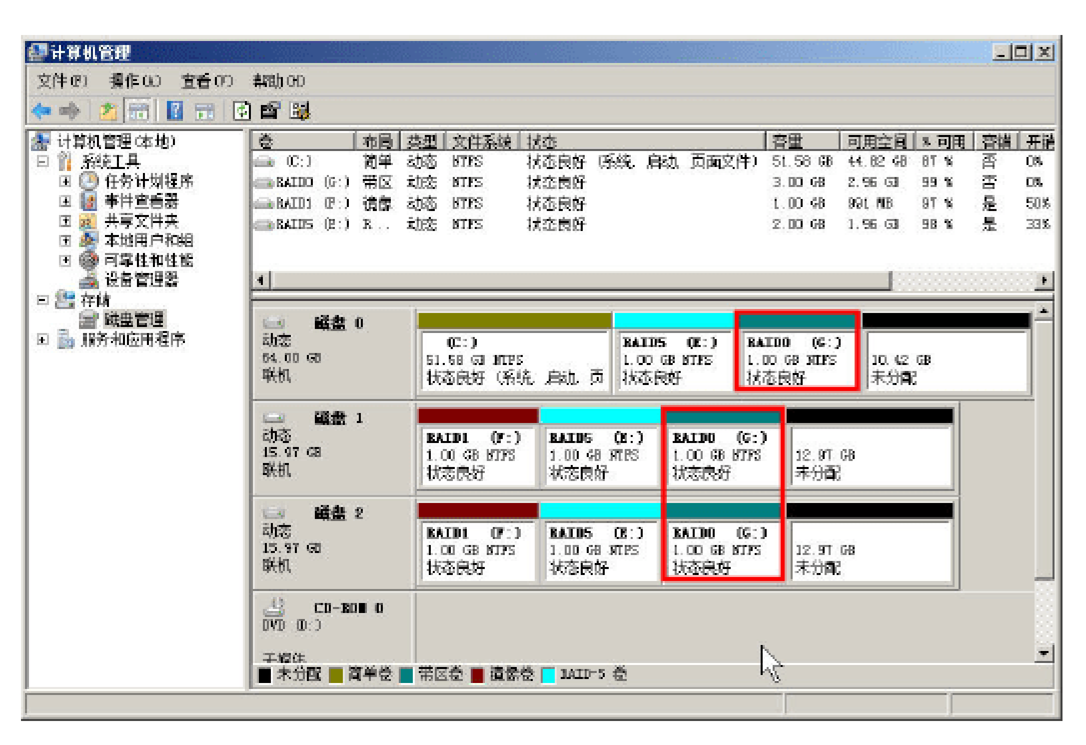
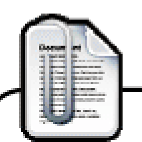


图 4-33　创建带区完成

4.3.6　创建跨区卷（对现有磁盘扩容）

跨区卷是由多个物理磁盘上的磁盘空间组成的卷。可以通过向其他动态磁盘扩展来增加跨区卷的容量。这一功能是非常有用的，比如，将 SQL Server 安装在 D 盘，随着数据库内容的增加，磁盘的可用空间很少，就可以使用“跨区卷”对 E 盘进行扩容。跨区卷只能在动态磁盘上创建，同时不能容错也不能被镜像。



说 明

如果服务器有硬件的 RAID 卡，但在使用 RAID 卡创建逻辑磁盘时，分配的逻辑磁盘比较少，并且安装了操作系统及应用程序。或者，在使用 RAID 卡创建的逻辑磁盘比较大，在安装操作系统的时候，创建了多个分区，每个分区容量比较少。这时候，就可以使用“跨区卷”功能，把这些小的分区“合并”。

在本次操作中，将创建一个“简单卷”，然后对其扩容，具体操作步骤如下所示。

01 在“磁盘管理”窗格中，右击“磁盘 0”的剩余空间，选择“新建简单卷”，如图 4-34 所示。

图 4-34　新建简单卷

02 然后根据向导，创建一个大小为 5000MB 的简单卷并用 NTFS 文件系统格式化，设置盘符为 H。

03 右击新创建的 H 卷，在弹出的快捷菜单中选择“扩展卷”命令，如图 4-35 所示。

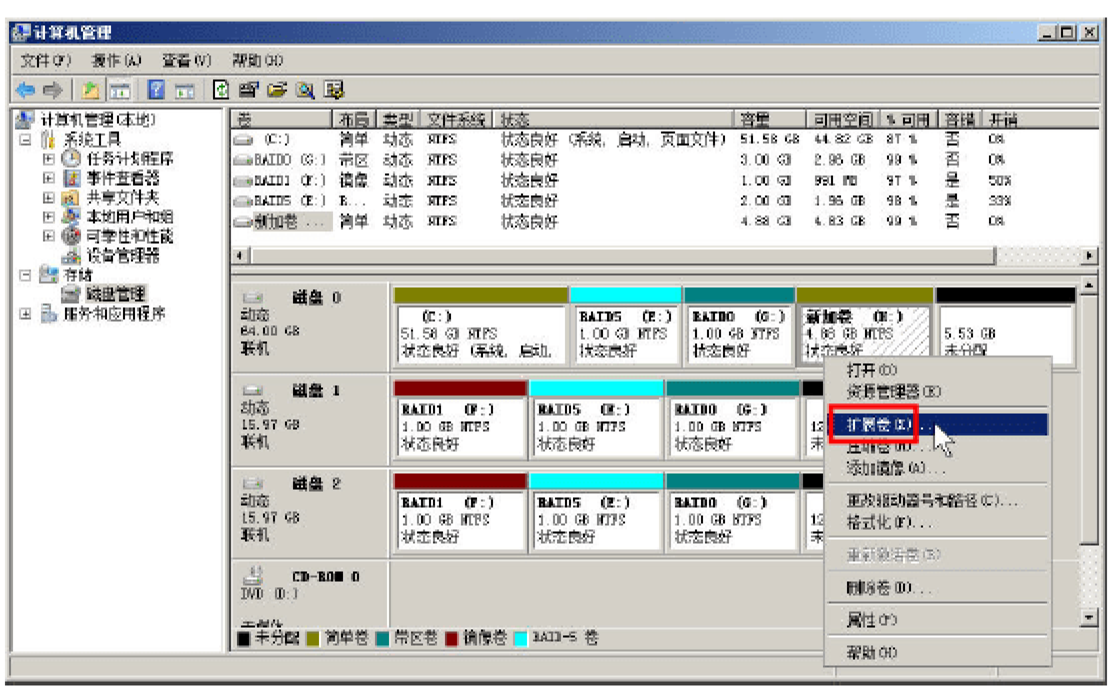


图 4-35　扩展卷

04 在“选择磁盘”对话框中，添加剩余的两块磁盘，并且分别为“磁盘 1”选择 1024MB，为“磁盘 2”选择 2048MB，磁盘 0 保持默认值（使用所有剩余的空间），如图 4-36 所示。

05 扩展卷完成后，用“玫红”色表示，如图 4-37 所示。



图 4-36　添加磁盘并指定每个磁盘上分配的空间

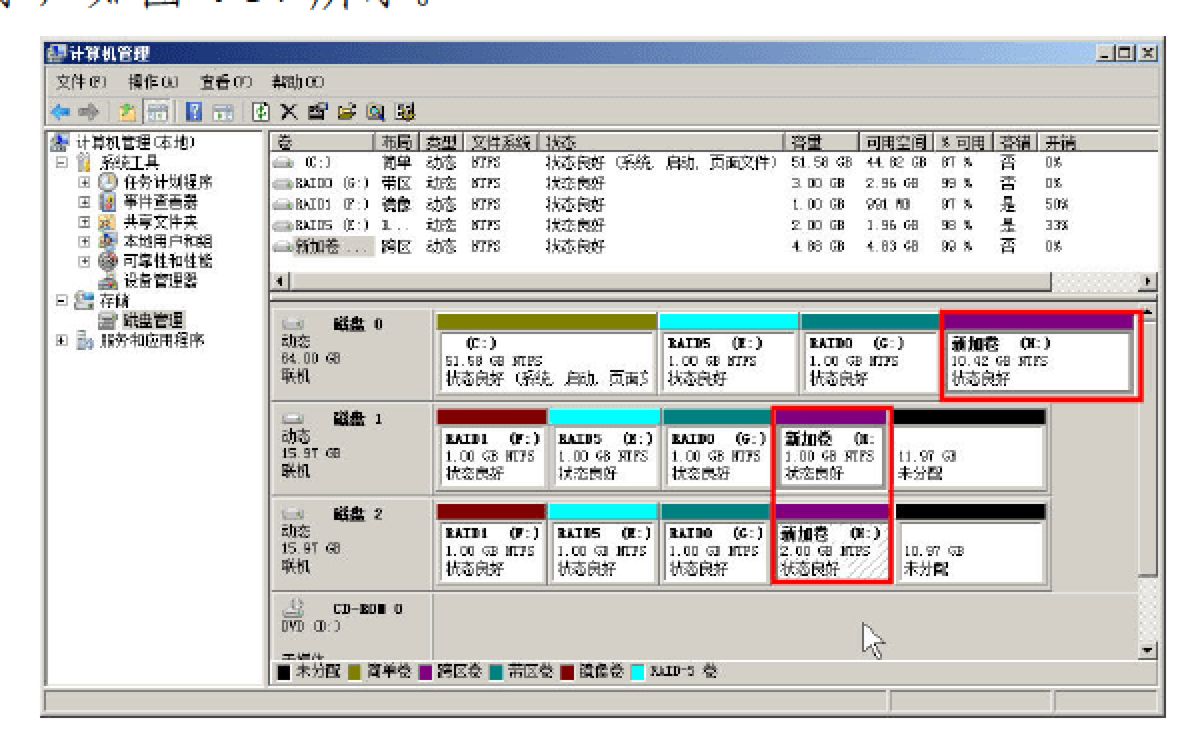


图 4-37　完成扩展

4.3.7　镜像卷、RAID5 卷、带区卷、跨区卷的安全性

在前几节所做的操作中，磁盘镜像和 RAID 5，当其中的一个硬盘损坏时，数据可以恢复。而

带区卷和跨区卷其中的一个硬盘损坏时，所有数据丢失并且不能恢复。所以，在创建带区卷、跨区卷时，如果要保持数据的安全性，只有这些卷所属的磁盘是采用底层陈列卡创建的 RAID5、RAID0、RAID50、RAID6 的“逻辑磁盘”时，才推荐采用。

在 Windows Server 2003、Windows Server 2008 中，要想修复 RAID 1、RAID 5 卷，需要删除失败的磁盘，然后再修复 RAID。这里只介绍修复 RAID 5 卷过程，修复 RAID 1 卷与此类似，具体操作步骤如下。

01 关闭 Windows Server 2008 虚拟机，为“磁盘 2”创建并选择一个新的虚拟磁盘，如图 4-38 所示。

02 启动并进入 Windows 2008 虚拟机，进入“磁盘管理”为添加的新硬盘进行初始化。初始化后，将新添加的“磁盘 2”转换成“动态磁盘”，如图 4-39 所示。

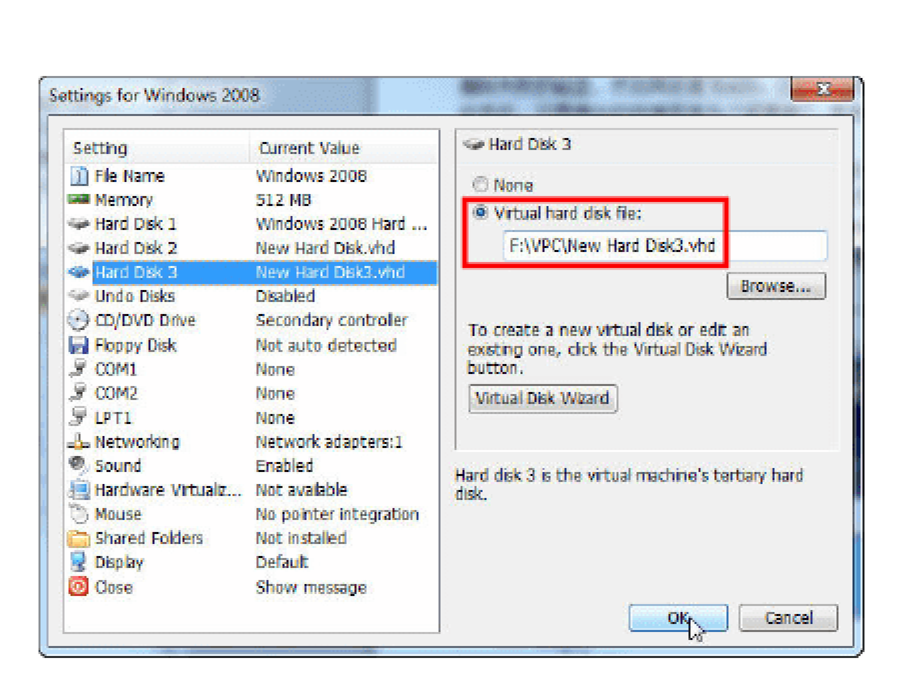


图 4-38　新建虚拟磁盘并选择

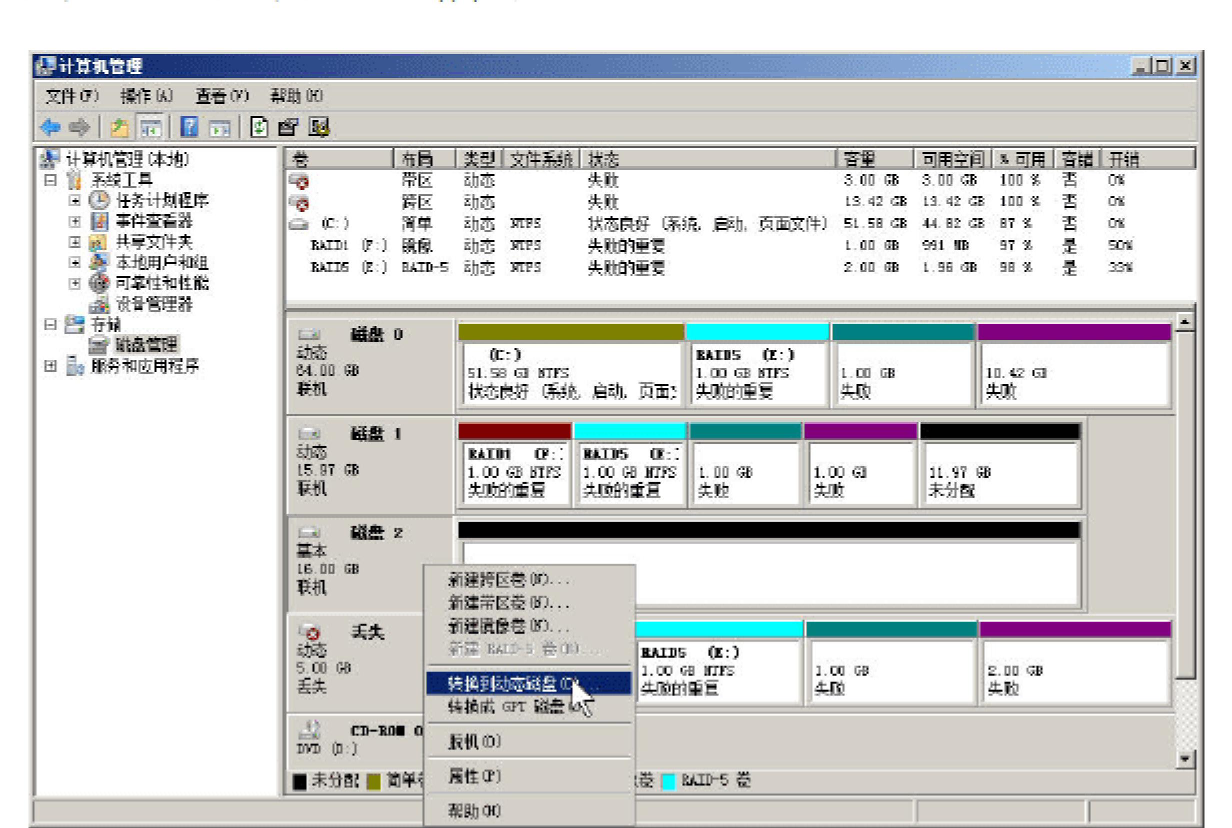


图 4-39　初始化并转换为动态磁盘

03 由于带区卷、跨区卷不可修复，所以可以将其删除，右击失败的跨区卷，在弹出的快捷菜单中选择“删除卷”命令，将其删除，如图 4-40 所示。同理，删除失败的带区卷。

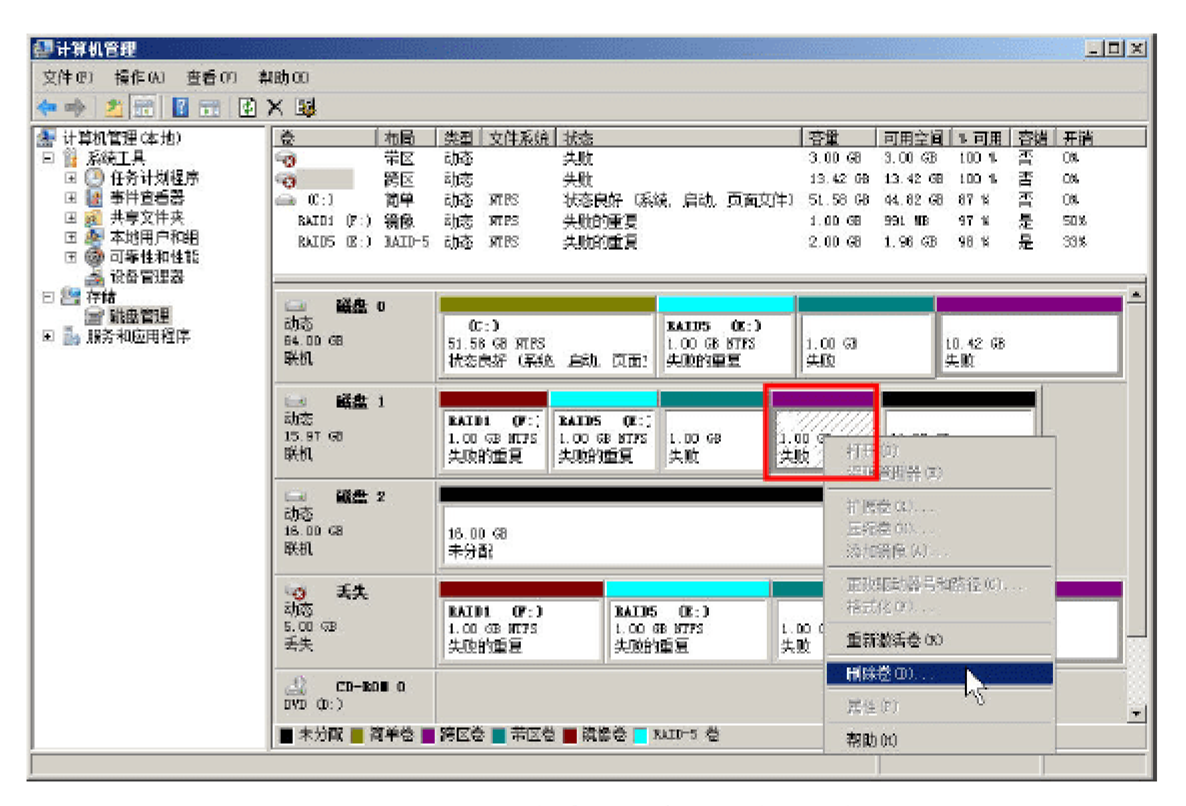


图 4-40　删除失败的跨区卷

04 右击 RAID5 卷，在弹出的快捷菜单中选择“修复卷”命令，如图 4-41 所示，单击“确定”按钮。

05 在弹出的“修复 RAID-5 卷”对话框中，选择“磁盘 2”用于修复，如图 4-42 所示。

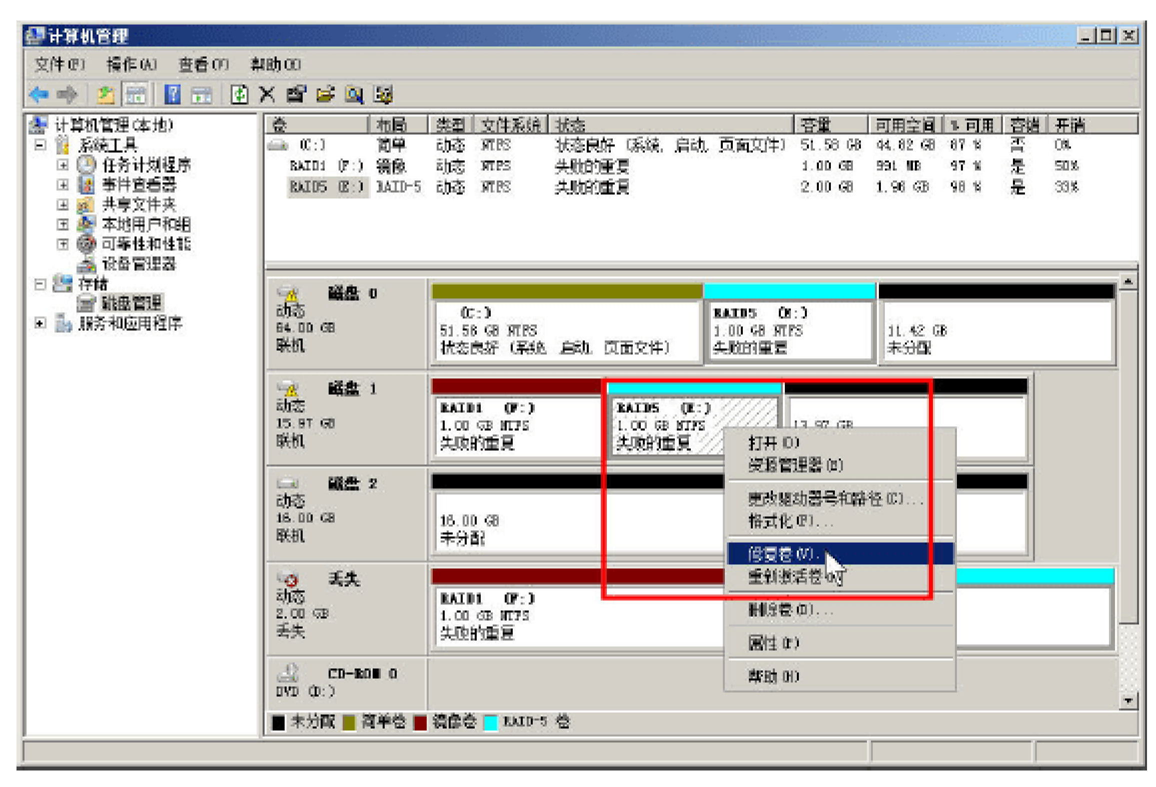


图 4-41　修复 RAID5 卷

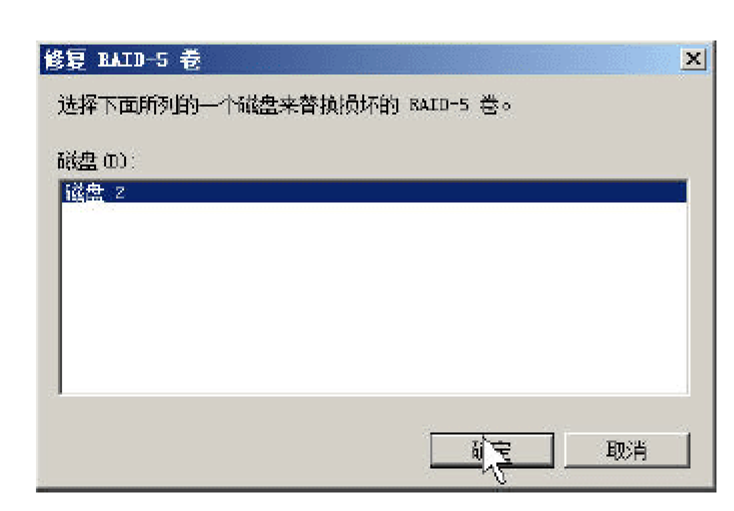


图 4-42　选择修复的磁盘

06 修复之后，如图 4-43 所示。

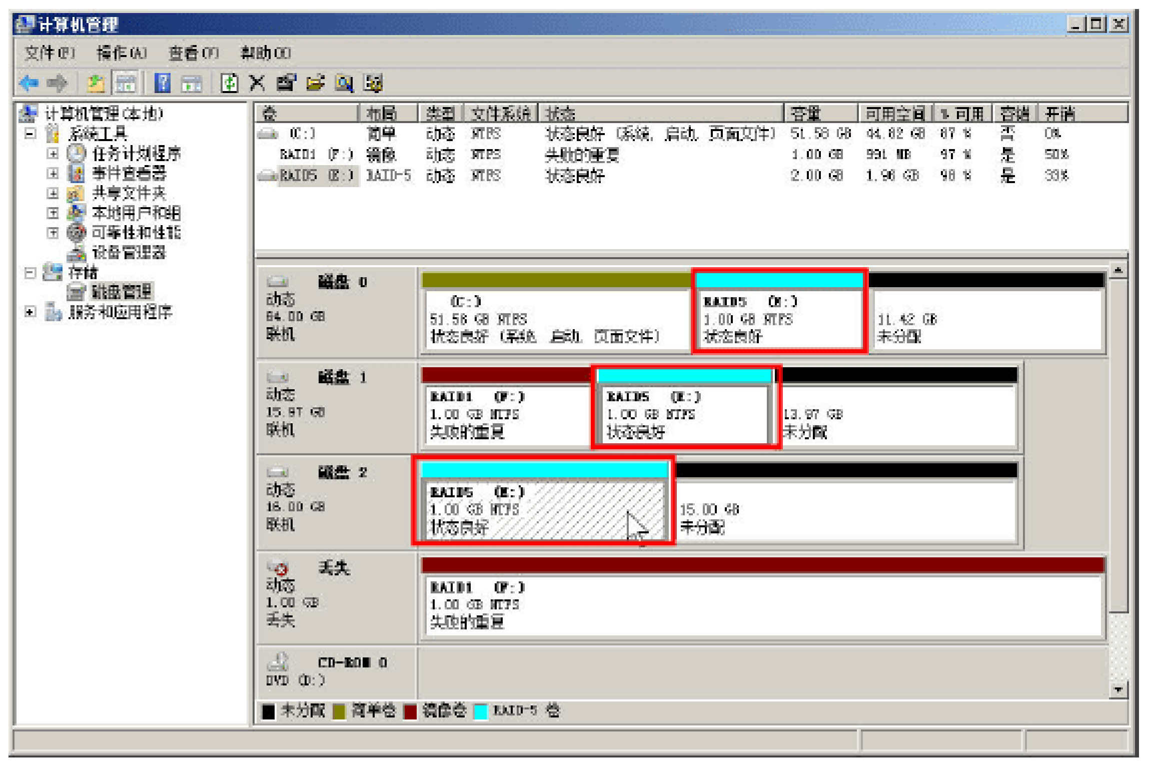


图 4-43　修复后的 RAID5 卷

4.3.8　恢复虚拟机的配置

在磁盘的实验完成之后，关闭 Windows 2008 虚拟机，并删除添加的第 2、第 3 块硬盘，只保留原来安装操作系统的硬盘。进入系统之后，删除以前做实验中创建的各卷，步骤如下。

01 关闭虚拟机，在虚拟机设置对话框中，只保留第 1 个硬盘，如图 4-44 所示。

02 进入“计算机管理→存储→磁盘管理”中，删除失败的 RAID5 卷，如图 4-45 所示。

03 然后关闭“计算机管理”，并重新进入“计算机管理→存储→磁盘管理”，右击“丢失”的磁盘，在弹出快捷菜单中选择

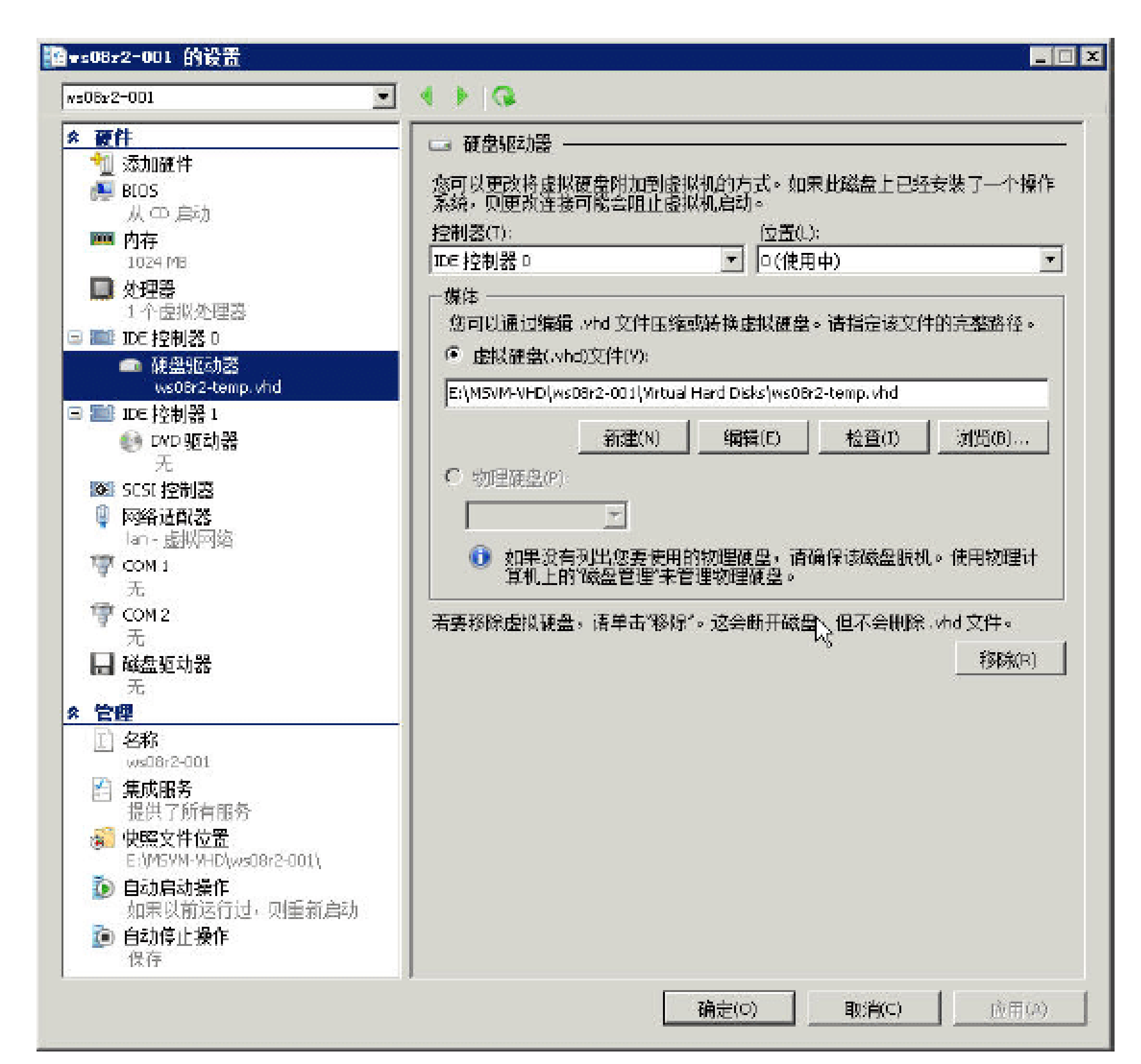


图 4-44　保留第一个硬盘

“删除磁盘”命令，如图 4-46 所示，删除丢失的磁盘。

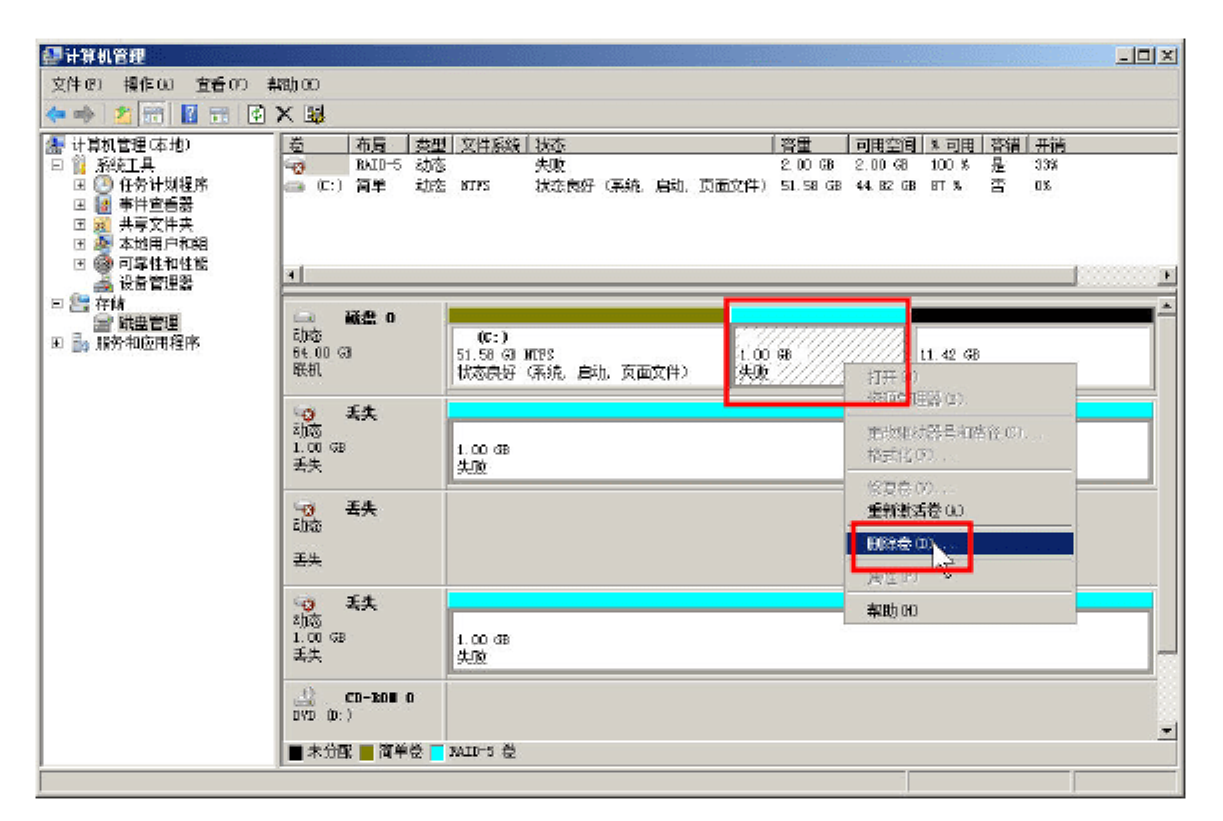


图 4-45　删除失败的 RAID5 卷

04 将所有丢失磁盘删除之后，在第 1 个磁盘剩余的空间，创建一个“简单卷”，并用 NTFS 文件系统格式化，在此设置盘符为 E，如图 4-47 所示，即可恢复虚拟机的配置。

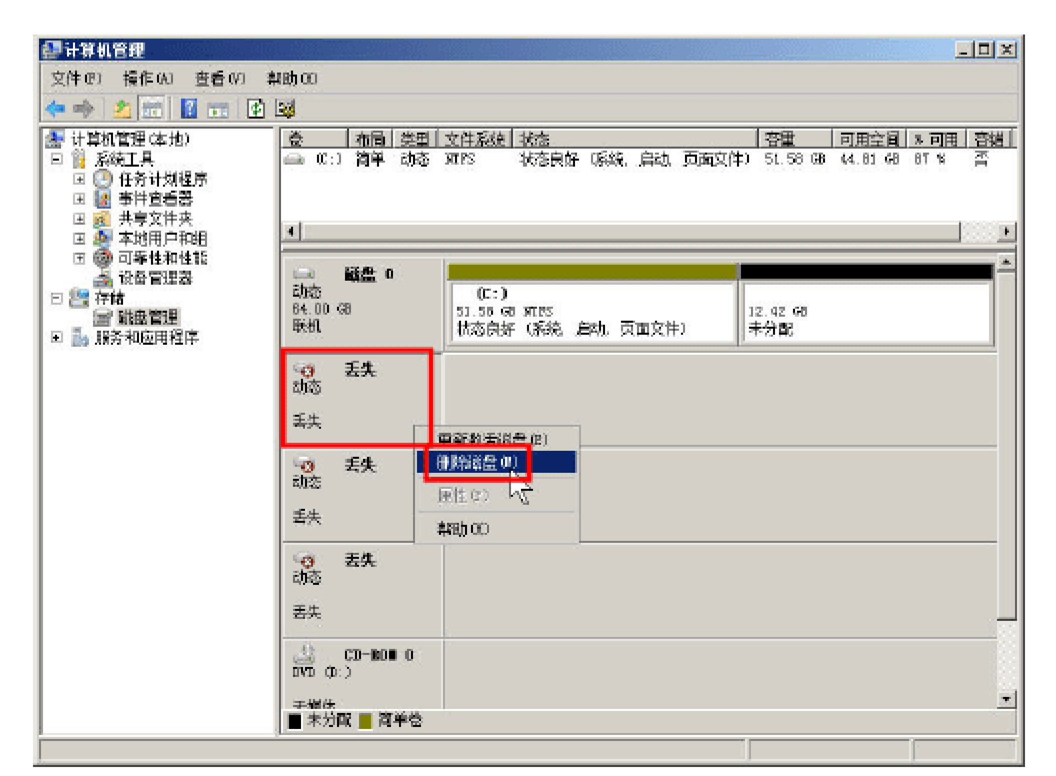


图 4-46　删除磁盘

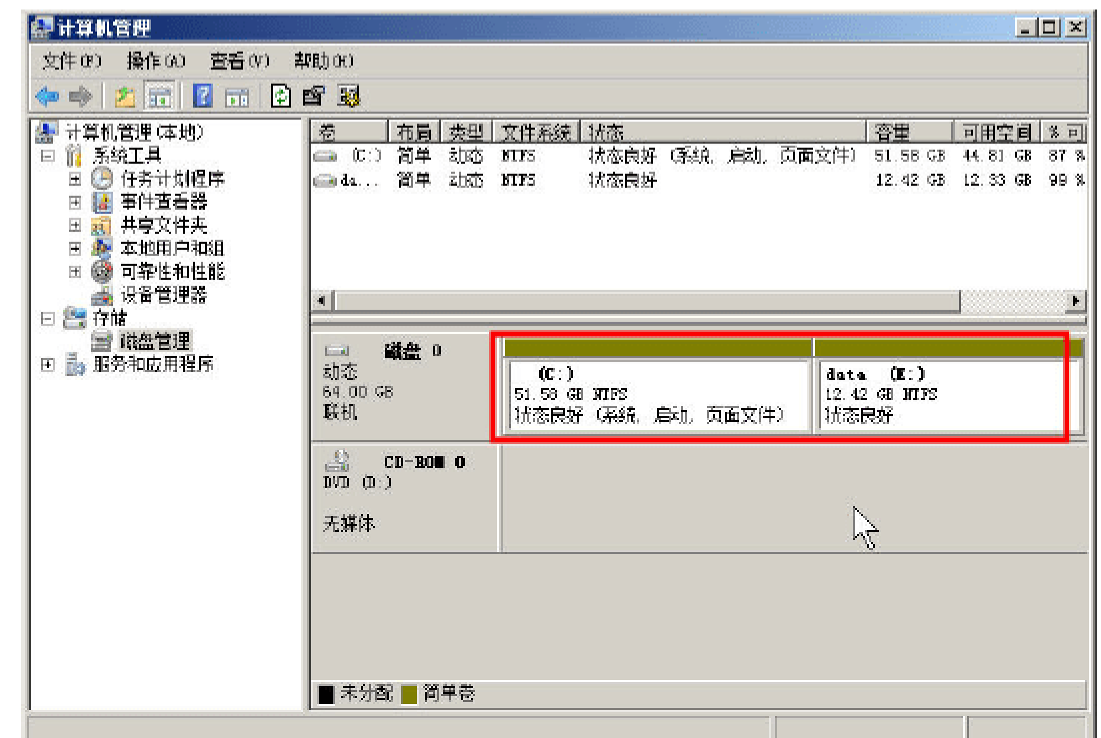


图 4-47　创建简单卷

4.4　NTFS 权限

权限是指与计算机上或网络上的对象（如文件和文件夹）关联的规则。权限确定是否可以访问某个对象以及可以对它执行哪些操作。例如，用户可能有访问网络上共享文件夹中文档的权限，但是只能读取该文档而不能对其进行更改。计算机上的系统管理员和具有管理员账户的用户可以为个人用户和组分配权限。

在前面的章节我们介绍了用户与用户组的概念，在本节中，将介绍 NTFS 文件系统的安全性，NTFS 安全是与用户、用户组配套使用的，单独介绍是没有意义的。

4.4.1　文件与文件夹权限

在每个文件系统中，都可以创建“文件”与“文件夹”（有时候也称为“目录”），所以，

NTFS 文件系统的权限也包括“文件”权限与“文件夹”权限。表 4-1 列出了文件和文件夹的权限级别。

表 4-1　NTFS 文件与文件夹权限级别

权限级别	描述
完全控制	用户可以查看文件或文件夹的内容，更改现有文件和文件夹，创建新文件和文件夹以及在文件夹中运行程序
修改	用户可以更改现有文件和文件夹，但不能创建新文件和文件夹
读取和执行	用户可以查看现有文件和文件夹的内容，并可以在文件夹中运行程序
读取	用户可以查看文件夹的内容，并可打开文件和文件夹
写入	用户可以创建新文件和文件夹，并对现有文件和文件夹进行更改

4.4.2　有效权限

在使用 NTFS 文件系统格式化的磁盘分区中，管理员可以对文件、文件夹进行多次的权限设置，并且设置的时候可以使用不同的用户与用户组，由于有的用户属于多个不同的用户组，则每个用户对于指定的文件或文件夹，可能具有多种权限的“混合”或“累加”，这时候就引出了“有效权限”的概念。对于“有效权限”，遵循以下三点：

- 拒绝一切：“拒绝”的权限优先级最高。用户对某个文件的有效权限是所有权限的累加之和，但只要其中有一个权限来源被设置为“拒绝”，则用户将不会拥有此权限。例如用户 user0001 属于 group001 组，假设用户 user0001 对某个文件夹（或文件）具有完全控制权限，而 group001 组对该文件夹的“读取”权限被设置为“拒绝”，则用户 user0001 也不能读取该文件夹。
- 权限累加：NTFS 权限是可以累加的。如果用户属于多个组，并且该用户与这些组分别对某个文件或文件夹拥有不同的权限设置时，则该用户的有效权限是所有权限来源的总和。
- 权限继承：NTFS 权限是可以继承的。在对文件夹设置权限后，该权限默认会被此文件夹下的“子文件夹”与“文件”继承。当然，也可以设置子文件夹不继承“父文件夹”的权限。

下面通过具体的实例介绍以上三点。

01 启动 Windows 2008 虚拟机，打开“资源管理器”窗口，打开 C 分区中的“用户→Administrator”文件夹，用鼠标右击，在弹出的快捷菜单中选择“属性”，如图 4-48 所示。

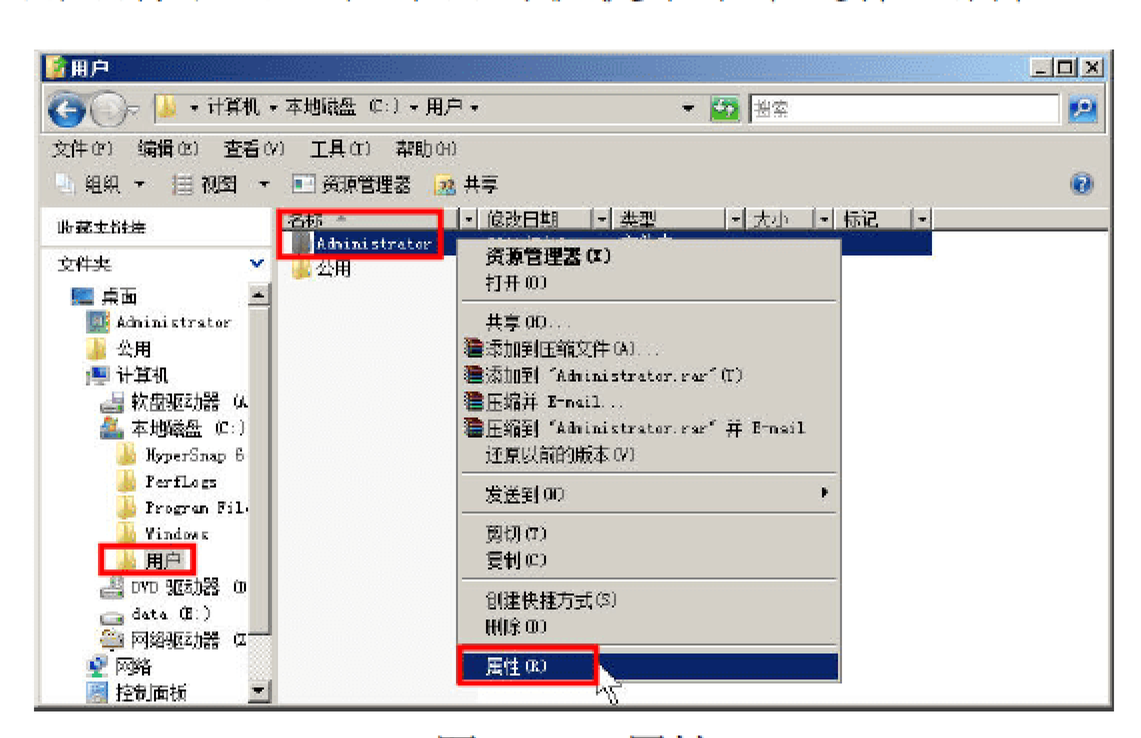


图 4-48　属性

02 打开“Administrator 属性”对话框，在“安全”选项卡中可以看到，当前文件夹添加了 2 个用户组（分别为 SYSTEM 和 Administrators）、1 个用户（Administrator），在“组或用户名”列表中，选择一个用户，例如 Administrator，则在正文窗格中显示对应账户（或组）的权限，如图 4-49 所示。

在图 4-49 中，当前的文件夹对 2 个用户组、1 个用户进行权限设置，由于 Administrator 用户属于 Administrators 组，则 Administrator 用户具有图 4-49 中，Administrator 用户及 Administrators 用户组的权限的“累加”。

03 如果想修改权限，例如添加其他用户或组对当前文件夹的权限，或者修改现有用户或组的权限，可以单击“编辑”按钮，在弹出的“Administrator 的权限”对话框中，在上方的窗格中，选中用户或组，在下方的窗格中对应的权限处确认（有✓者为选中，无✓者表示没有对应权限或权限不明），也可以单击“删除”按钮，删除选中用户或组的权限，或者单击“添加”按钮，添加用户或组，并在添加用户或组之后，选中新添加的用户和组，在下文的窗格中添加权限。在下方的权限窗格中，包括“允许”与“拒绝”两列权限，通常在“允许”一列中选择对应的权限，如果在“拒绝”一列中进行选择，则“拒绝”的权限将超过允许的权限，如图 4-50 所示。

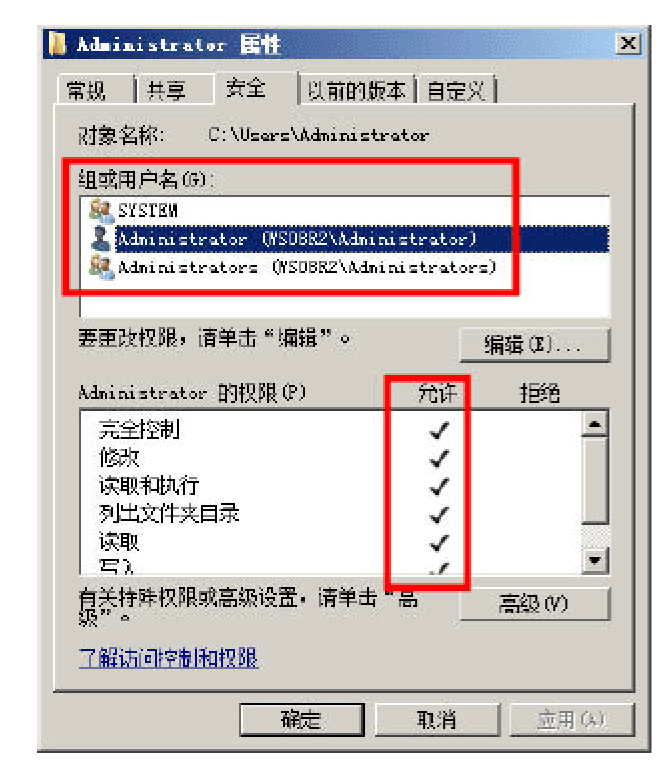



图 4-49　用户权限

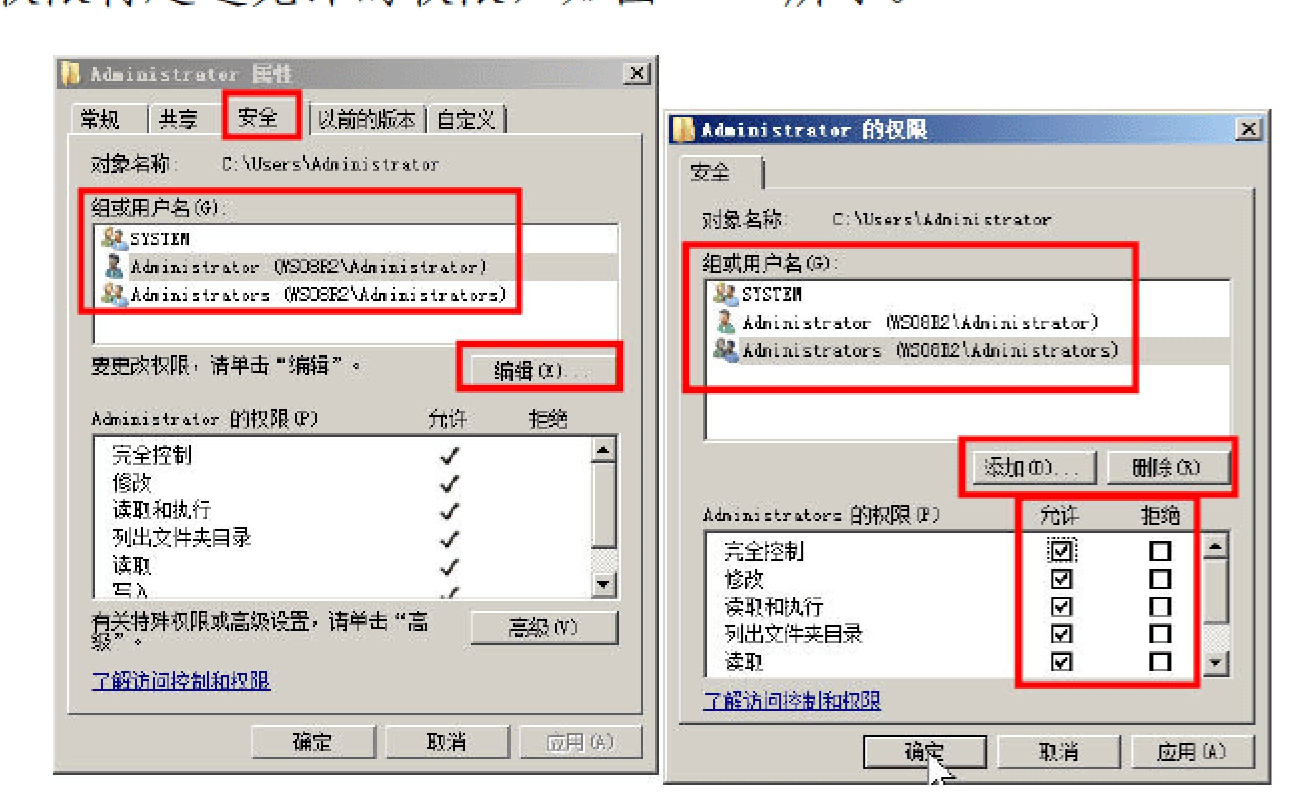


图 4-50　权限列表



说 明

不要修改“用户→Administrator”文件夹的权限，如果大家想练习权限，可在其他分区的其他文件夹中练习。

04 在 E 分区新建一个文件夹 test，并打开该文件夹的“安全”选项卡，单击“高级”按钮，在“test 的高级安全设置”对话框中，显示了继承权限，在“继承于”列表中显示了每个用户从那个文件夹继承来的权限，单击“编辑”按钮，可以修改继承权限，或者选择不继承，如图 4-51 所示。

05 在“有效权限”选项卡中，可以显示选中用户的有效权限。单击“选择”按钮，选择一个用户，在“有效权限”列表中，显示了该用户对此文件夹（或文件）的有效权限，如图 4-52 所示。

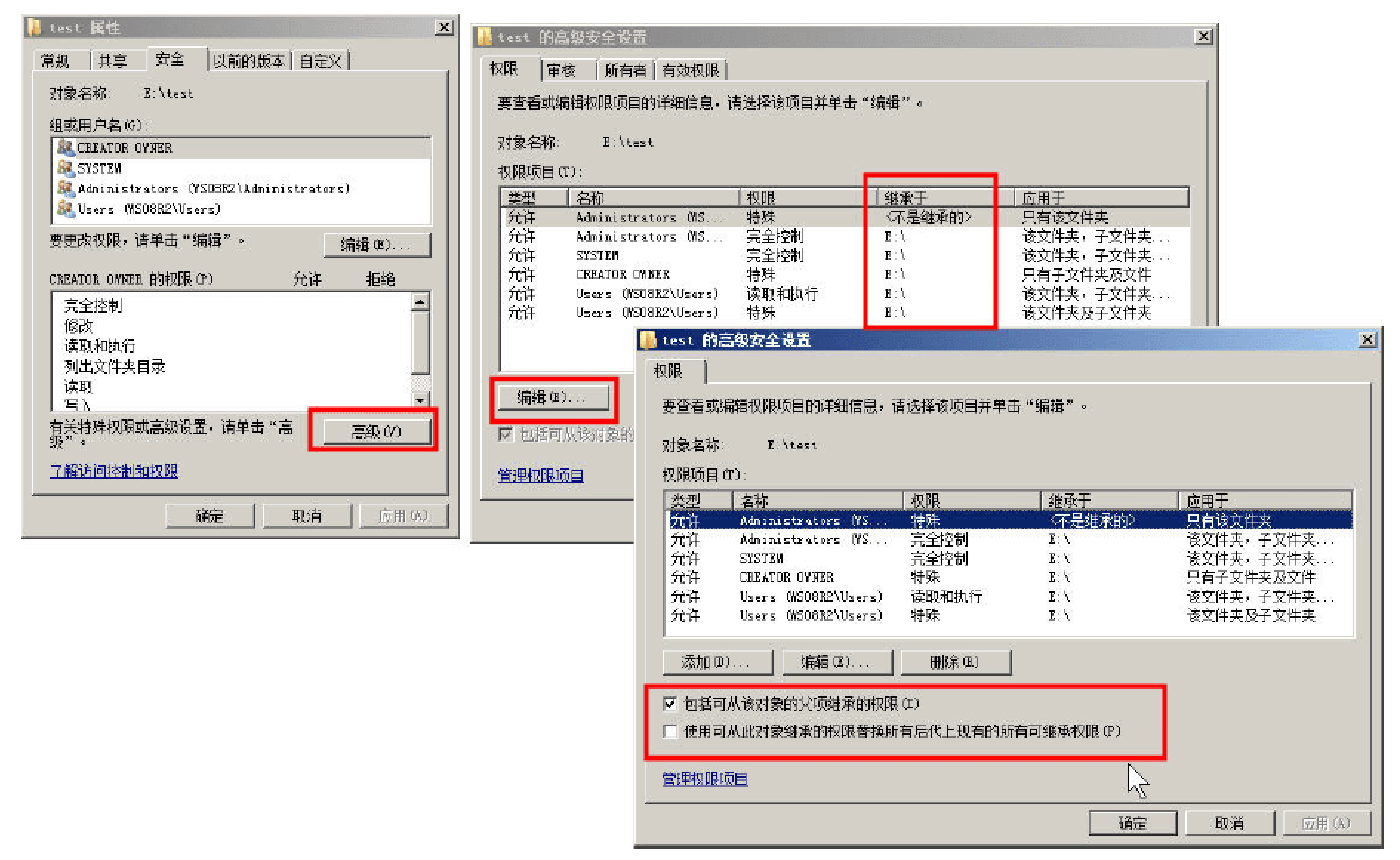


图 4-51　继承权限

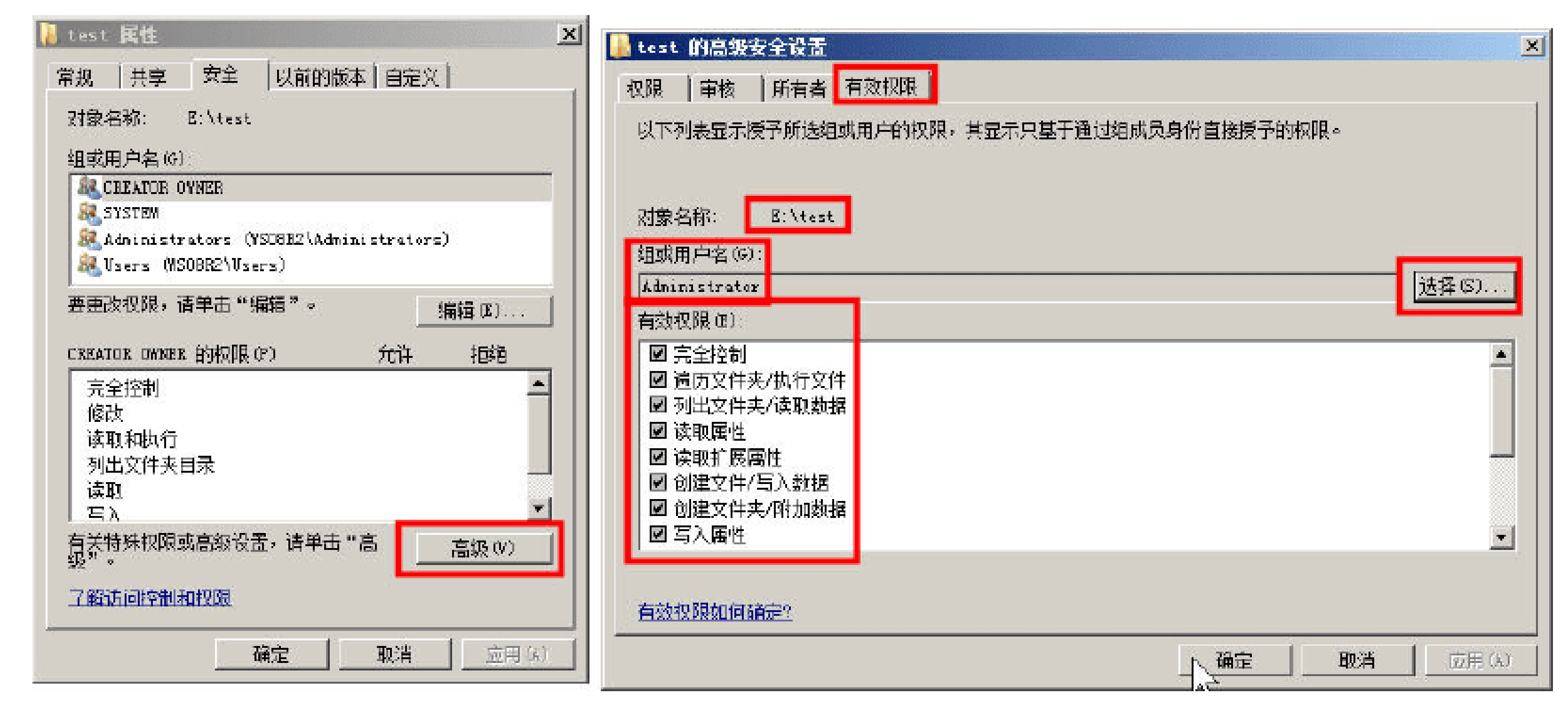


图 4-52　显示有效权限

4.4.3　文件或文件夹的所有权

NTFS 文件系统中每个文件与文件夹都有“所有者”，默认情况下，创建文件或文件夹的用户，就是该文件或文件夹的所有者。所有者可以更改其所拥有的文件或文件夹的权限，而管理员或具有管理员权限的用户，可以“取得”所有者权限。

打开一个文件夹的“高级安全设置”对话框，在“所有者”选项卡中，显示了当前的所有者，如果要修改所有者，请单击“编辑”按钮，在弹出的对话框中，单击“其他用户或组”对话框，添加用户或组，添加之后，在“将所有者更改为”列表中，选择用户或组，单击“确定”按钮既可完成更改，如图 4-53 所示。如果要替换子目录用户的所有者，请同时选中“替换子容器和对象的所有者”。

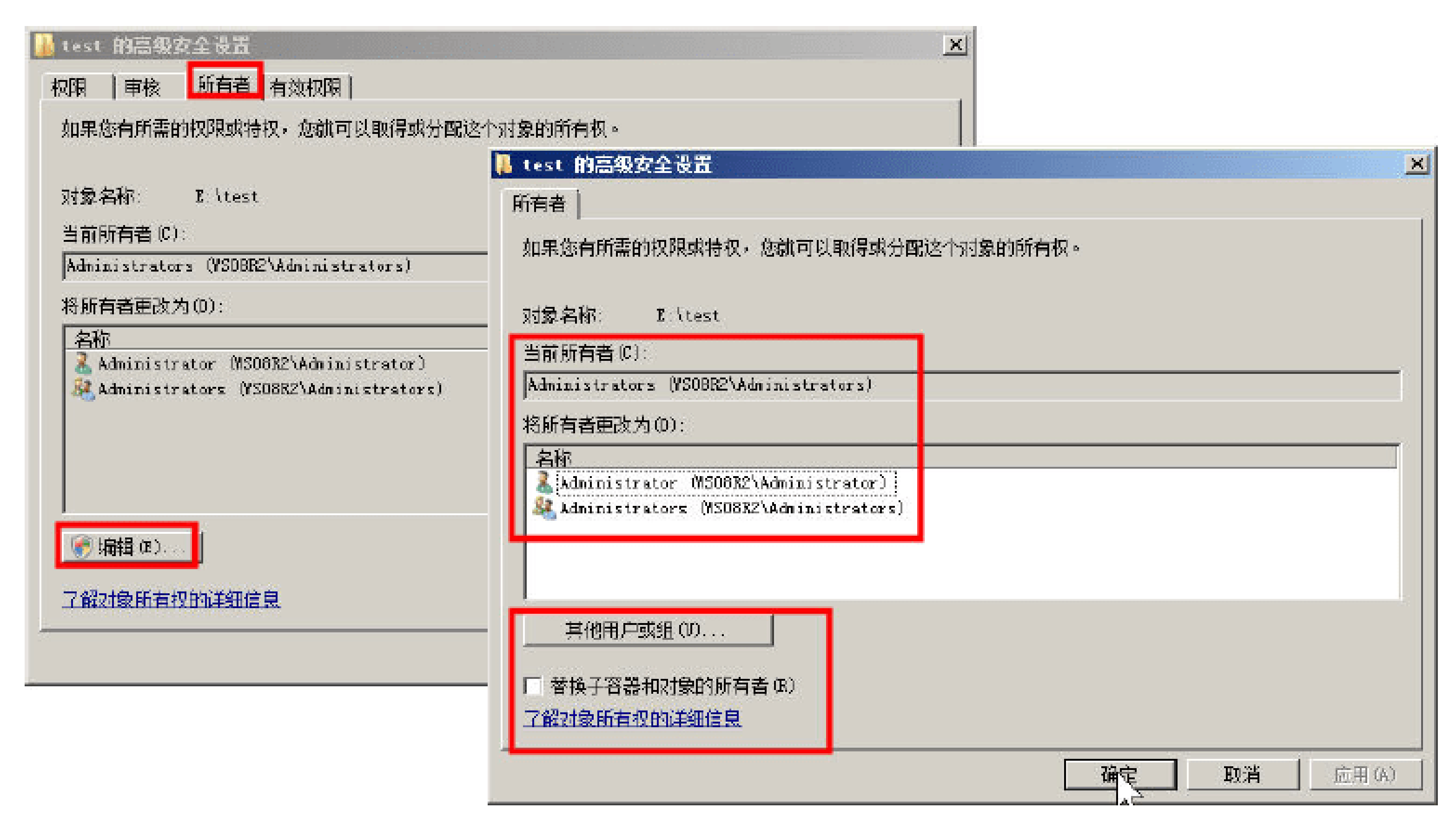


图 4-53　所有者权限

4.5　NTFS 压缩与加密

NTFS 文件系统还支持“压缩”与“加密”功能，采用压缩后，可以减少磁盘空间的占用；而采用加密的文件，其他用户不能查看其内容。不能对同一个文件或文件夹同时启用压缩与加密功能，二者只能使用其一。

4.5.1　NTFS 压缩

向 E 盘的 test 文件夹中复制一些文件与文件夹，然后测试其“压缩”功能，操作步骤如下。

01 右击 test 文件夹，在弹出的快捷菜单中选择“属性”命令，在“常规”选项卡中，单击“高级”按钮，如图 4-54 所示。

在“常规”选项卡中，在“大小”处，显示了所选的文件夹的大小，本例中为 13.0MB，在“占用空间”处显示了占用的磁盘空间，本例为 13.4MB。

02 在弹出的“高级属性”对话框中，选中“压缩文件内容以使节省磁盘空间”复选框，然后单击“确定”按钮，如图 4-55 所示。

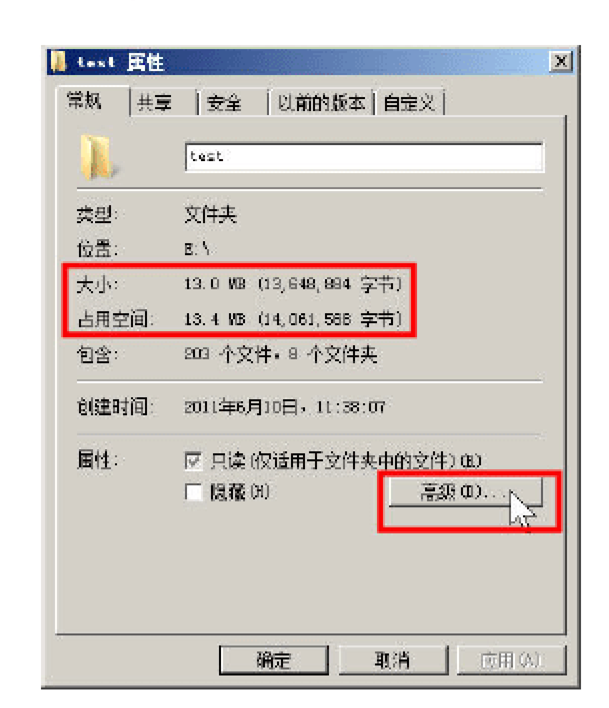


图 4-54　常规属性

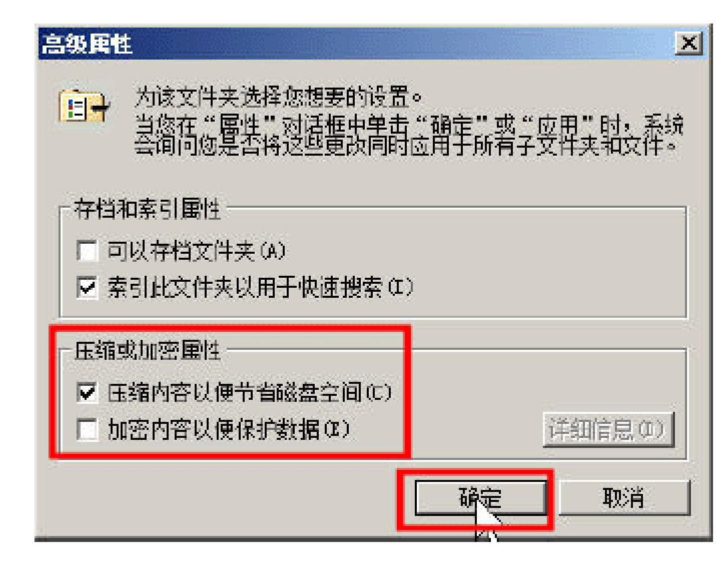


图 4-55　压缩文件内容

03 返回到图 4-54 的“常规”选项卡后，单击“确定”按钮。会弹出“确认属性更改”对话框，选中“将更改应用于此文件夹、子文件夹和文件”，然后单击“确定”按钮，开始压缩，如图 4-56 所示。

04 压缩完成后，再次打开该文件夹属性，在“大小”处显示文件夹大小仍然为 13.0MB，而“占用空间”大小则改为 11.5MB，比原来的 13.4MB 小了 1.9MB，这是压缩之后节省的磁盘空间，如图 4-57 所示。

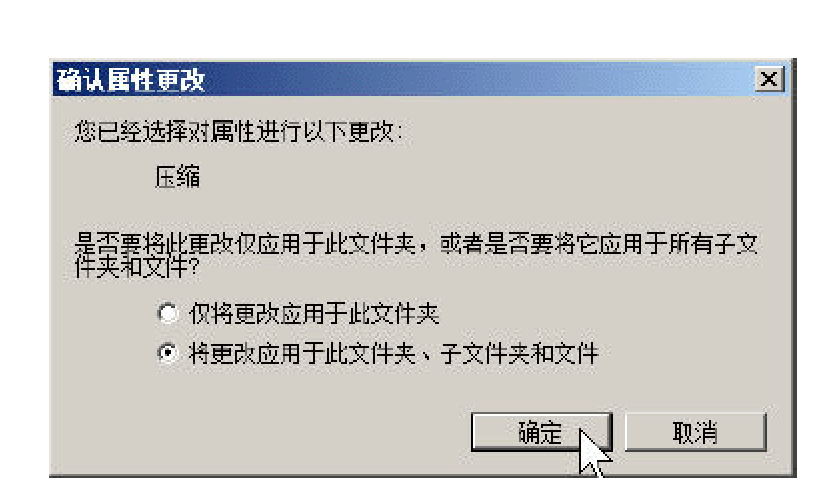


图 4-56　确认压缩属性

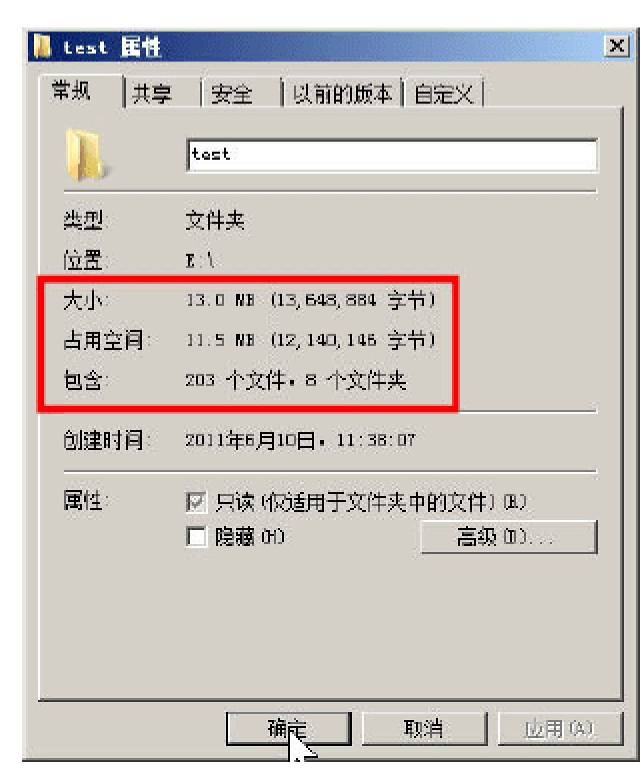


图 4-57　压缩后占用空间变小

4.5.2　加密文件系统

“加密文件系统（Encrypting File System，简称 EFS）”提供文件加密的功能，文件经过加密后，只有当初将其加密的用户或被授权的用户才能够读取。

> **说　明**
>
> 重新安装操作系统，对于压缩的文件，可以由管理员解压缩。对于不具有“有效权限”的文件或文件夹，可以由管理员通过“取得所有权”操作，获得或更改所有权。但使用 EFS 加密的文件，在重新安装操作系统后，如果没有备份原加密用户的密钥，则加密的文件将不能打开。所以，EFS 具有相当高的安全性。

01 打开 test 文件夹的属性，在“高级属性”对话框中，选中“加密内容以便保护数据”复选框，然后单击“确定”→“确定”按钮，如图 4-58 所示。

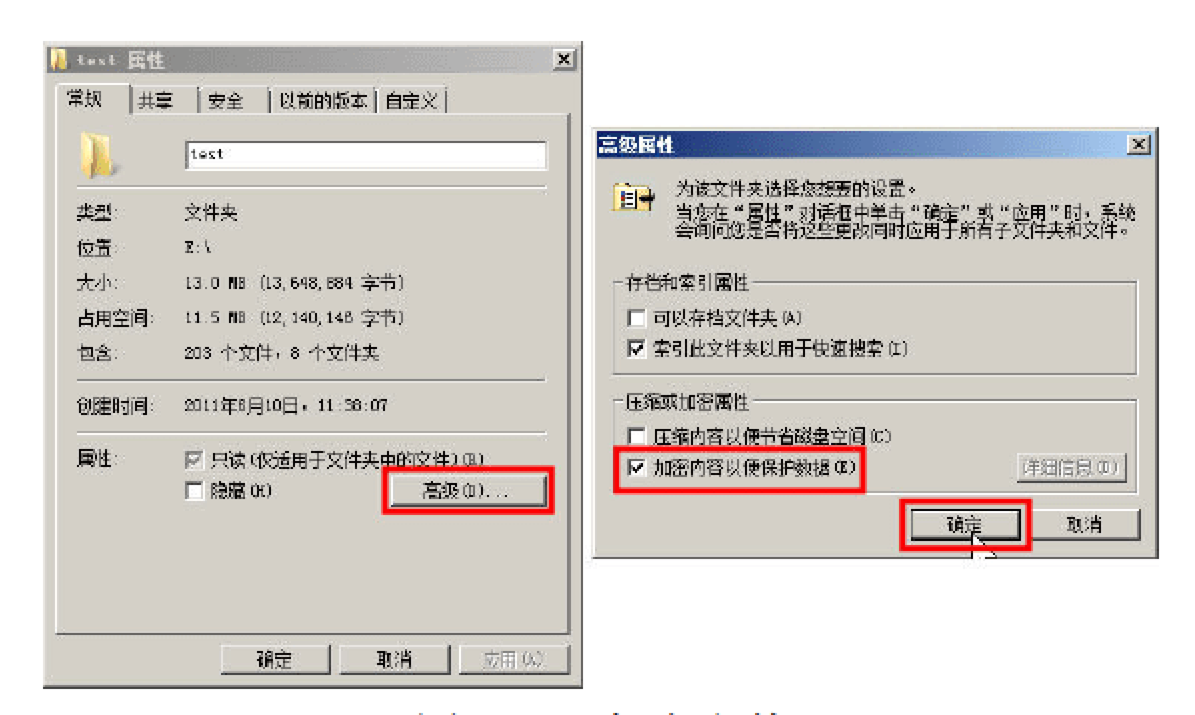


图 4-58　加密文件

02 在弹出的“确认属性更改”对话框中，单击“确定”按钮，如图 4-59 所示。

03 在将文件加密之后，其他用户可以复制（如果有读取权限）加密后的文件或文件夹，但不能打开文件查看其内容。

04 如果要“解密”或“解压缩”文件或文件夹，可以在图 4-55 或图 4-58 中，取消选中“压缩内容以便节省磁盘空间”或“加密内容以便保护数据”的选项既可。

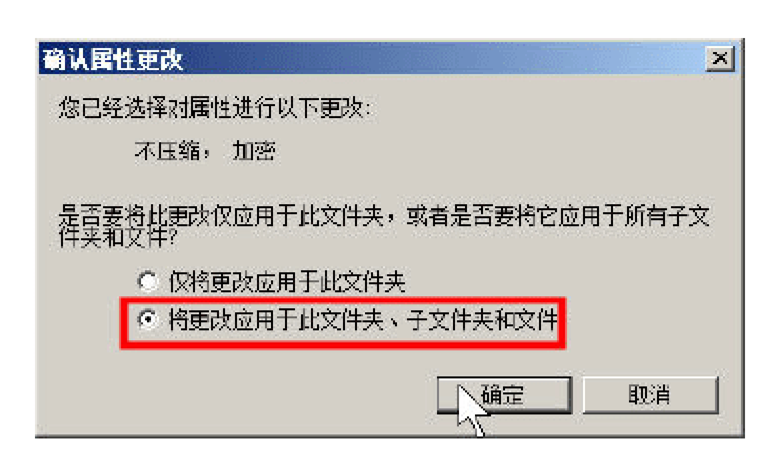


图 4-59　确认加密

4.5.3　备份 EFS 加密证书

如果对计算机上的数据进行了加密，则当加密密钥出现意外情况时，而又无法恢复数据时，该数据将会丢失。若要确保始终可以访问加密数据，应当将加密密钥进行备份。备份 EFS 加密密钥（证书）的步骤如下。

01 从“开始”菜单打开“运行”对话框，输入 certmgr.msc，然后按回车键，如图 4-60 所示。

02 定位到“证书-当前用户→个人→证书”，在右侧选中 EFS 加密证书，单击鼠标右键，在弹出的快捷菜单中选择“所有任务→导出”命令，如图 4-61 所示。

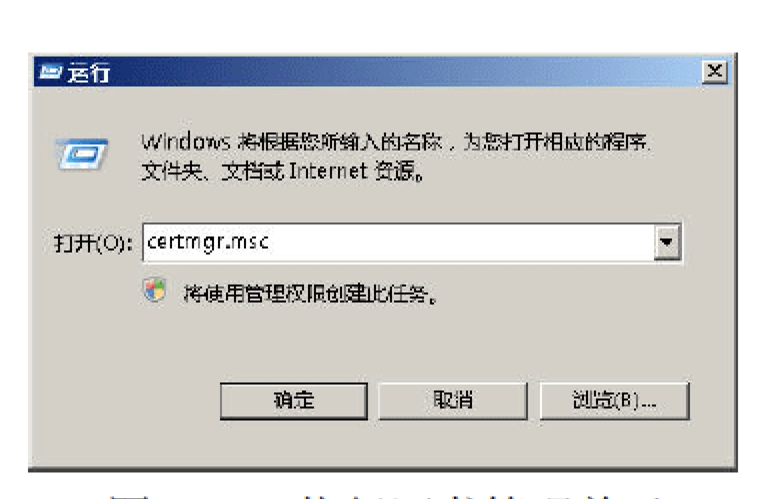


图 4-60　执行证书管理单元

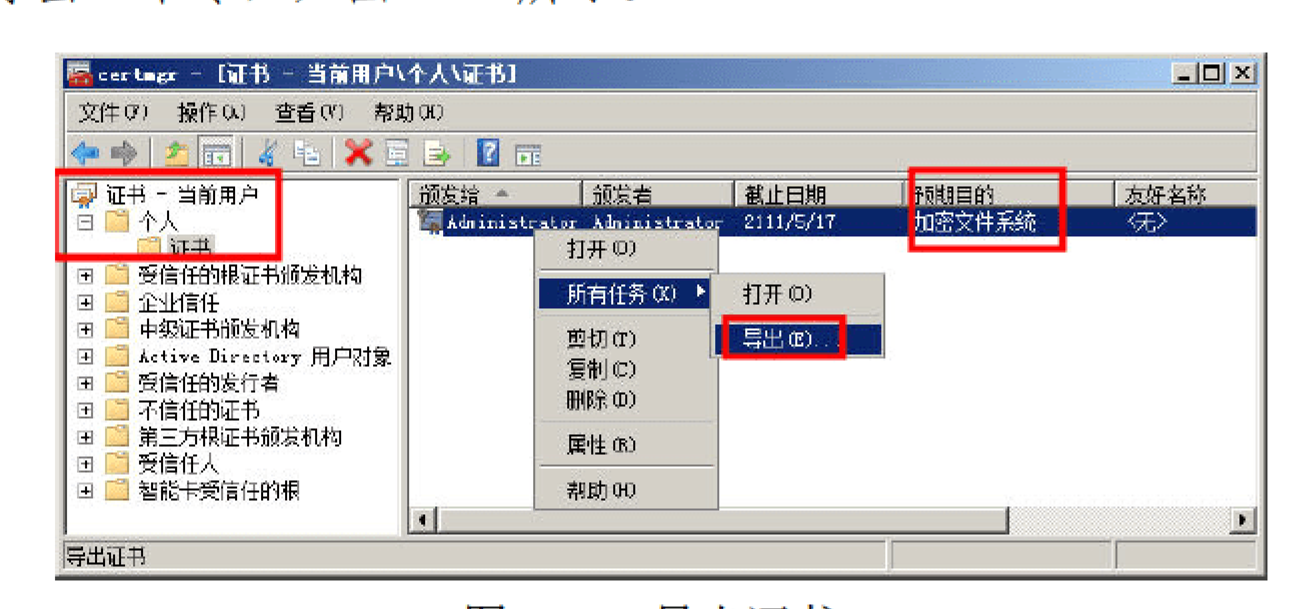


图 4-61　导出证书

03 在“导出私钥”对话框，选中“是，导出私钥”单选按钮，如图 4-62 所示。

04 在“导出文件格式”对话框，选择默认值。

05 在“密码”对话框，输入并确认密码，以后将使用该密码导入证书，如图 4-63 所示。

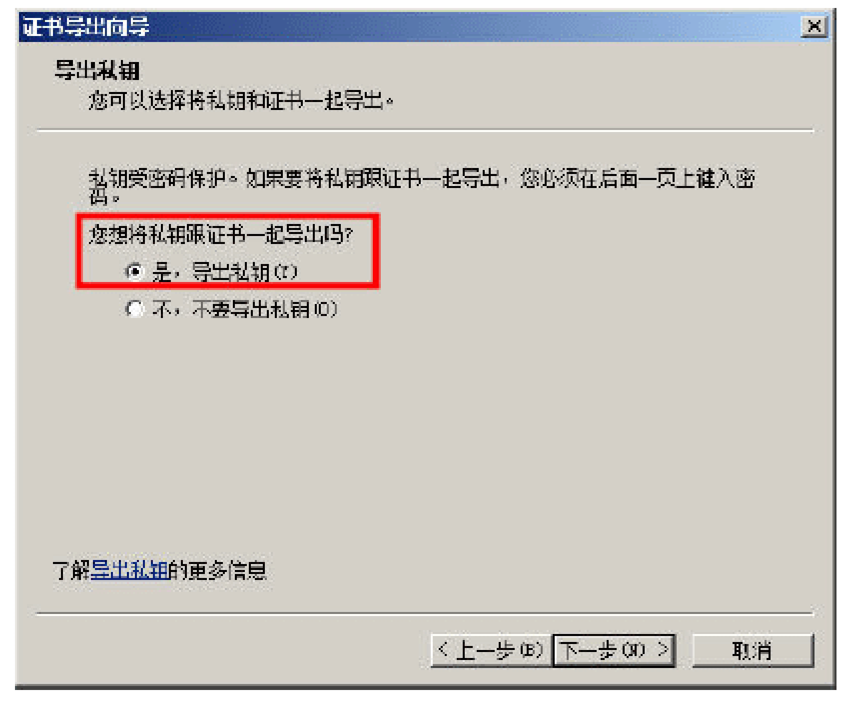


图 4-62　导出私钥

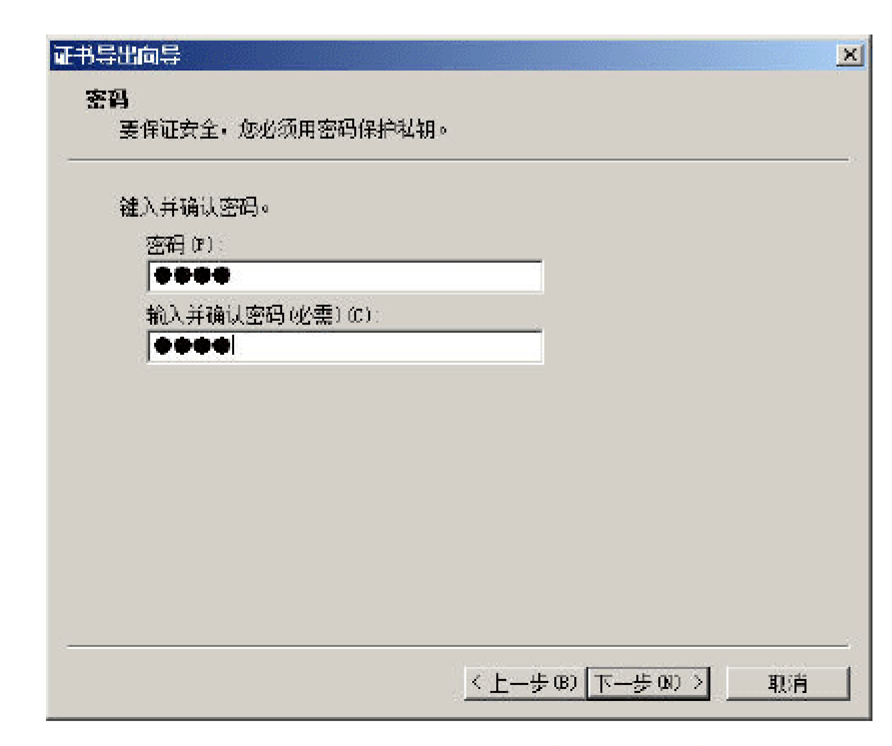


图 4-63　设置密码保护证书

06 在“要导出的文件”对话框，为导出的证书指定一个文件名并选择保存路径，如图 4-64

所示。

07 证书导出完成后，将图 4-64 中的文件保存到安全的位置，建议将该文件压缩并保存到多个不同的位置，例如，保存在邮箱的网络存储中、保存到其他计算机中等。

08 如果采用 EFS 加密的文件（或文件夹）所属的操作系统出现问题，重新安装后，如果要“打开”或“解密”EFS 加密文件，则应打开证书管理单元，在右侧窗格中选择“所有任务→导入”命令（如图 4-65 所示），然后导入图 4-64 中导出的文件既可。

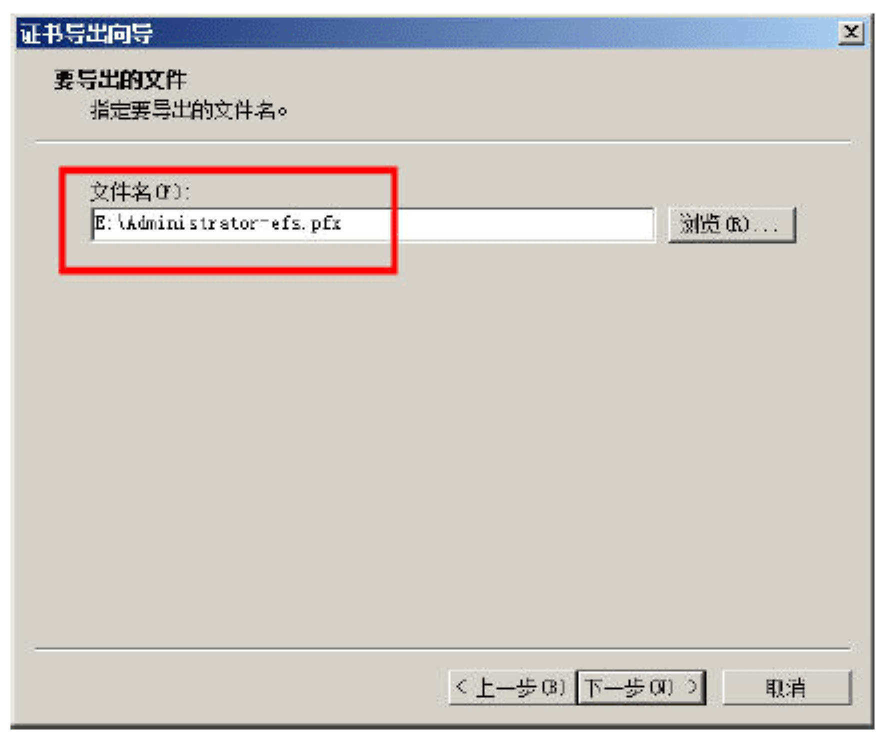


图 4-64　指定证书导出文件名及保存路径

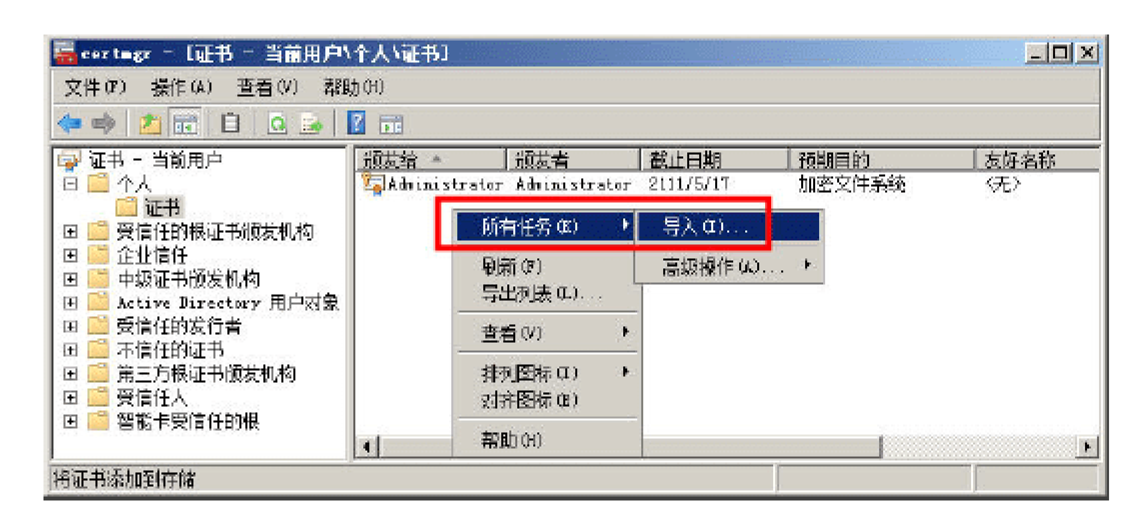


图 4-65　导入 EFS 证书

4.6　Bit Locker 驱动器加密

Windows BitLocker 驱动器加密是用于客户端计算机的 Windows Vista、Windows 7 以及 Windows Server 2008 、Windows Server 2008 R2 操作系统中的一项可用的数据保护功能。Windows BitLocker 驱动器加密是一项加密功能，可用于对计算机附加的一个或多个卷（驱动器）进行加密，还可以使用受信任的平台模块（TPM）来验证早期启动组件的完整性。

4.6.1　BitLocker 的硬件和软件需求

以下是使用 BitLocker 需满足的条件。

- 运行 Windows Vista、Windows 7 的企业版、旗舰版或 Windows Server 2008 、Windows Server 2008 R2 的计算机。
- 正常操作的受信任的平台模块（TPM）微芯片版本 1.2 或安全的可移动 USB 设备。
- 与受信任计算组（TCG）兼容的 BIOS。
- 两个 NTFS 驱动器分区，一个用于系统卷，一个用于操作系统卷。
- 首先从硬盘驱动器（而不是 USB 或 CD 驱动器）启动计算机的 BIOS 设置。

由于 BitLocker 对整个数据卷进行加密，所以需要为计算机配置用于启动的活动分区，该分区将从操作系统卷中独立出来，这称为“负载拆分配置”。用户数据存储在操作系统卷或其他数据卷上，这些卷也可以通过 BitLocker 进行加密。

4.6.2 BitLocker 与 EFS 的区别

BitLocker 驱动器加密和 EFS 加密文件系统之间有许多不同之处。BitLocker 专门用于计算机被盗或未经授权的用户试图访问计算机时，保护安装 Windows 驱动器上的所有个人文件和系统文件。EFS 以每个用户为基础，保护任何驱动器上的单独文件。表 4-2 显示了 BitLocker 驱动器加密和 EFS 之间的主要不同之处。

表 4-2 BitLocker 与 EFS 之间的主要不同之处

BitLocker 驱动器加密	EFS 加密文件系统
BitLocker 将加密安装 Windows 的驱动器上的所有个人文件和系统文件	EFS 将加密任何驱动器上的单独文件
BitLocker 并不依赖与文件关联的单独用户账户。BitLocker 适用于所有用户或组	EFS 将根据与其关联的用户账户来加密文件。如果计算机具有多个用户或组，则每个用户（或组）可以单独加密各自的文件
BitLocker 使用受信任的平台模块（TPM），该模块是某些新型计算机中一种支持高级安全功能的特殊微芯片	EFS 并不需要（或不使用）任何特殊硬件
启用 BitLocker 加密之后，只有管理员才能打开或关闭 BitLocker 加密	而使用 EFS 则不必具有管理员身份

可以同时使用 BitLocker 驱动器加密和加密文件系统获取由这两种功能提供的保护。在使用 EFS 时，加密密钥将与计算机的操作系统一同存储。尽管进行了加密，但如果黑客能够启动或访问系统驱动器，则使用该加密方式仍可能存在危险。如果将 BitLocker 安装在另一台计算机上，则使用 BitLocker 对系统驱动器进行加密会防止启动或访问系统驱动器，从而帮助保护这些密钥。

4.6.3 添加 BitLocker 功能

使用 BitLocker 驱动器加密的时候，由于在系统启动时，需要读取 TPM 或 USB 设备，而目前的许多虚拟机软件（VMware Workstation、Windows Virtual PC）不支持在系统启动前使用 USB 设备，所以，不能在虚拟机中做这个实验。在本节中，将在物理主机上安装 Windows Server 2008 R2，并为系统卷（安装 Windows 操作系统的分区）添加 BitLocker。如果在非系统卷（例如 D 盘、E 盘）启用 BitLocker，则不需要 TPM 或 USB 设备，所以可以在虚拟机中做非系统卷的 BitLocker 实验。

01 使用管理员账户登录 Windows Server 2008 R2，进入“服务器管理器→存储→磁盘管理”中，可以看到有 1 个 100MB 的“系统保留”分区，以及安装 Windows Server 2008 R2 的系统卷（大约 33.03GB），如图 4-66 所示。这符合 BitLocker 驱动器加密 对“磁盘分区”的要求。

02 运行 gpedit.msc，打开“本地组策略编辑器”，定位到“计算机配置→管理模板→Windows 组件→BitLocker 驱动器加密→操作系统驱动器”，双击右侧的“启动时需要附加身份验证”命令，如图 4-67 所示。

03 在打开的“启动时需要附加身份验证”对话框中，选中“已启用”单选按钮，并选中“没有兼容的 TPM 时允许 BitLocker”复选框，这样，如果没有 TPM 芯片的计算机，可以用 U 盘代替 TPM 芯片，如图 4-68 所示。设置之后单击“确定”按钮，然后关闭本地组策略编辑器。

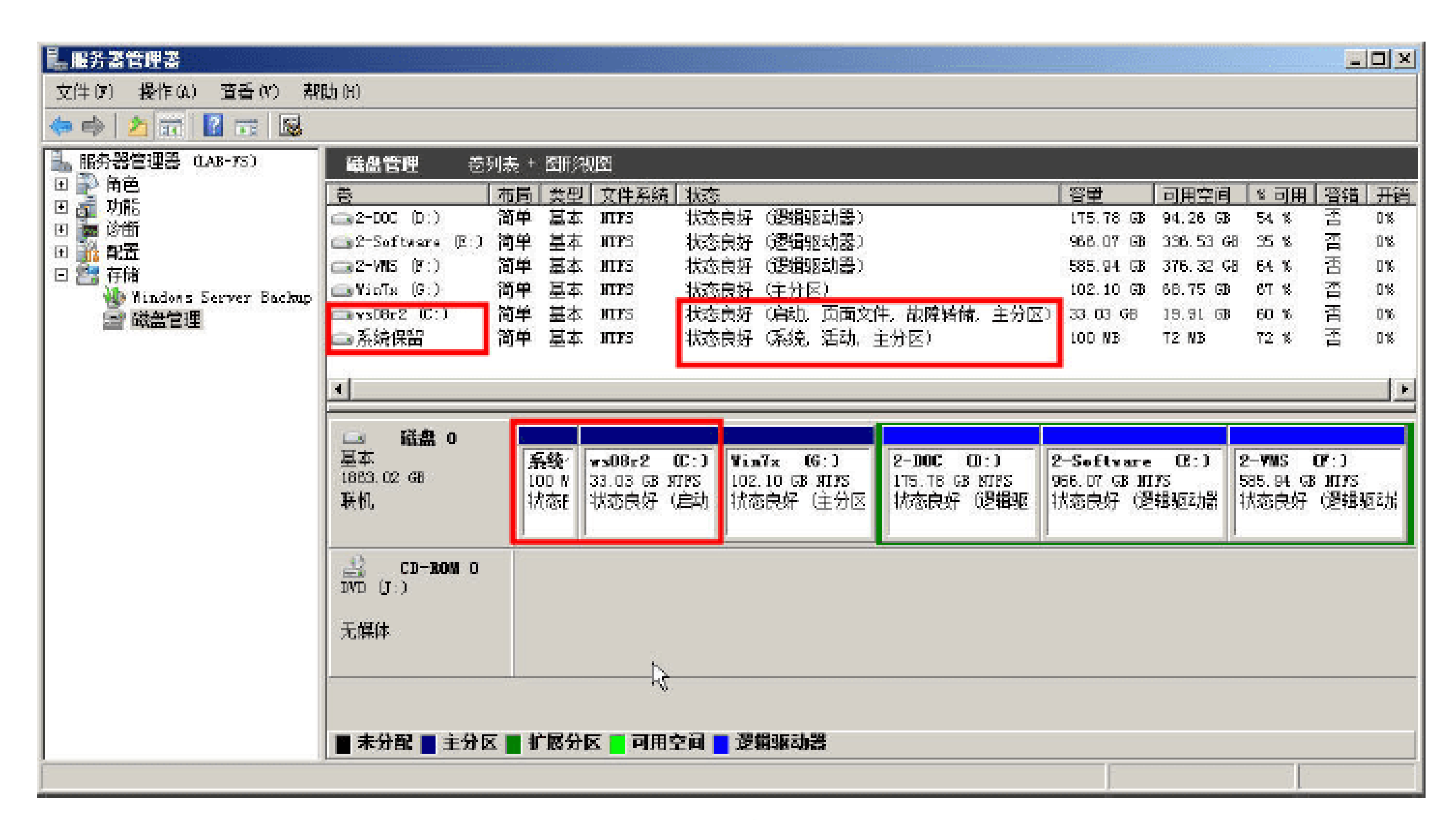


图 4-66　磁盘分区列表

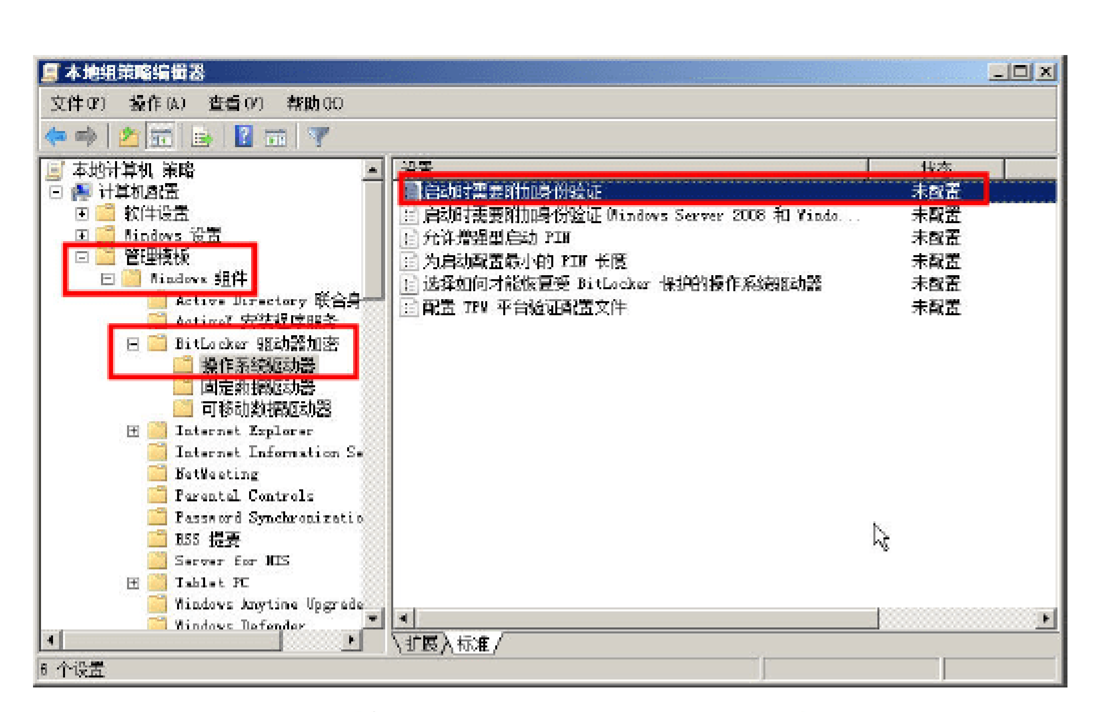


图 4-67　修改 BitLocker 驱动器加密策略

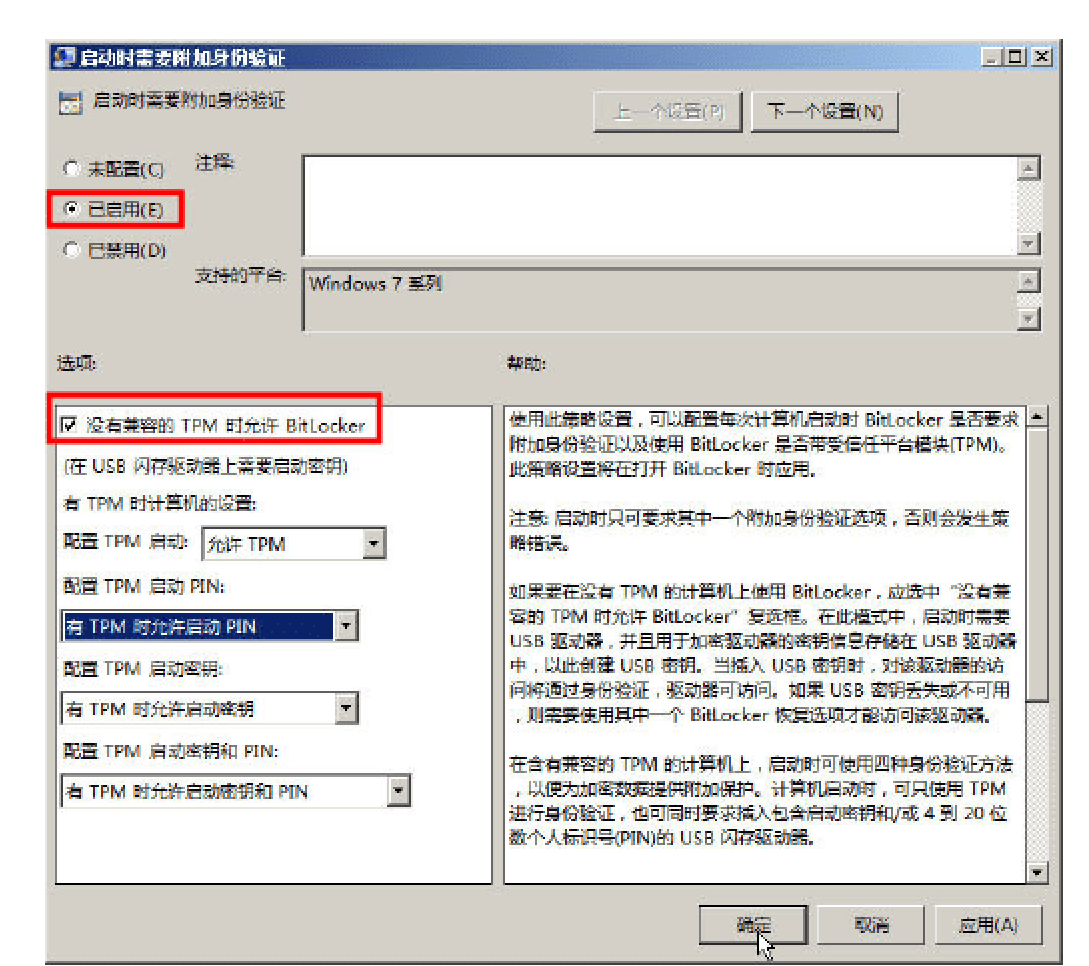


图 4-68　启用 U 盘启用 BitLocker 功能

04 打开“服务器管理器”窗口，右击“功能”，在弹出的快捷菜单中选择“添加功能”命令，或者在“功能”列表中单击“添加功能”链接，如图 4-69 所示。

05 在“选择功能”对话框中，选中“BitLocker 驱动器加密”复选框，如图 4-70 所示。

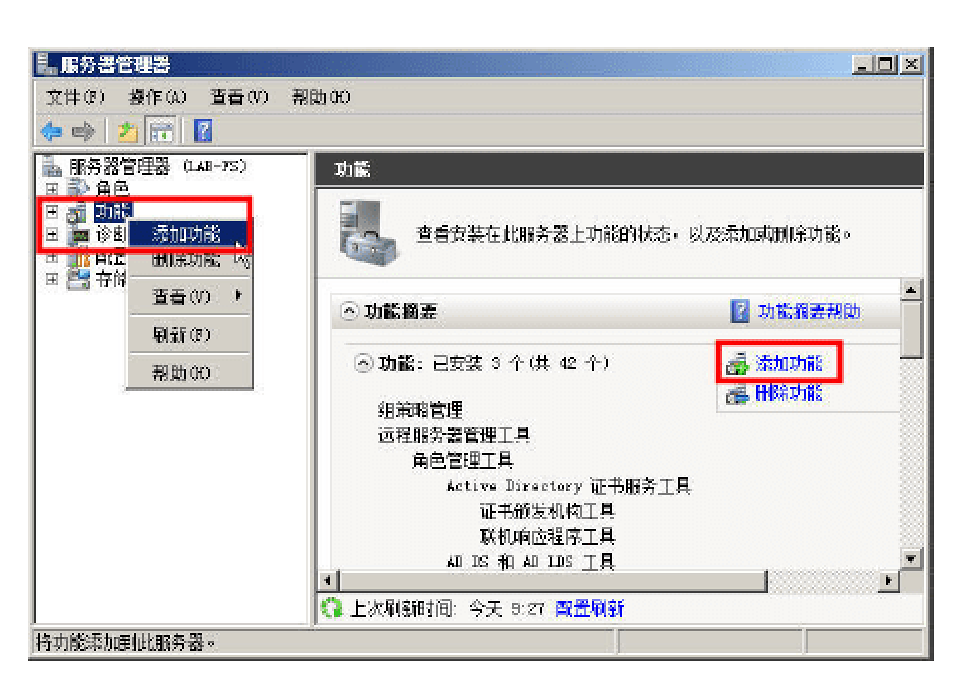


图 4-69　添加功能

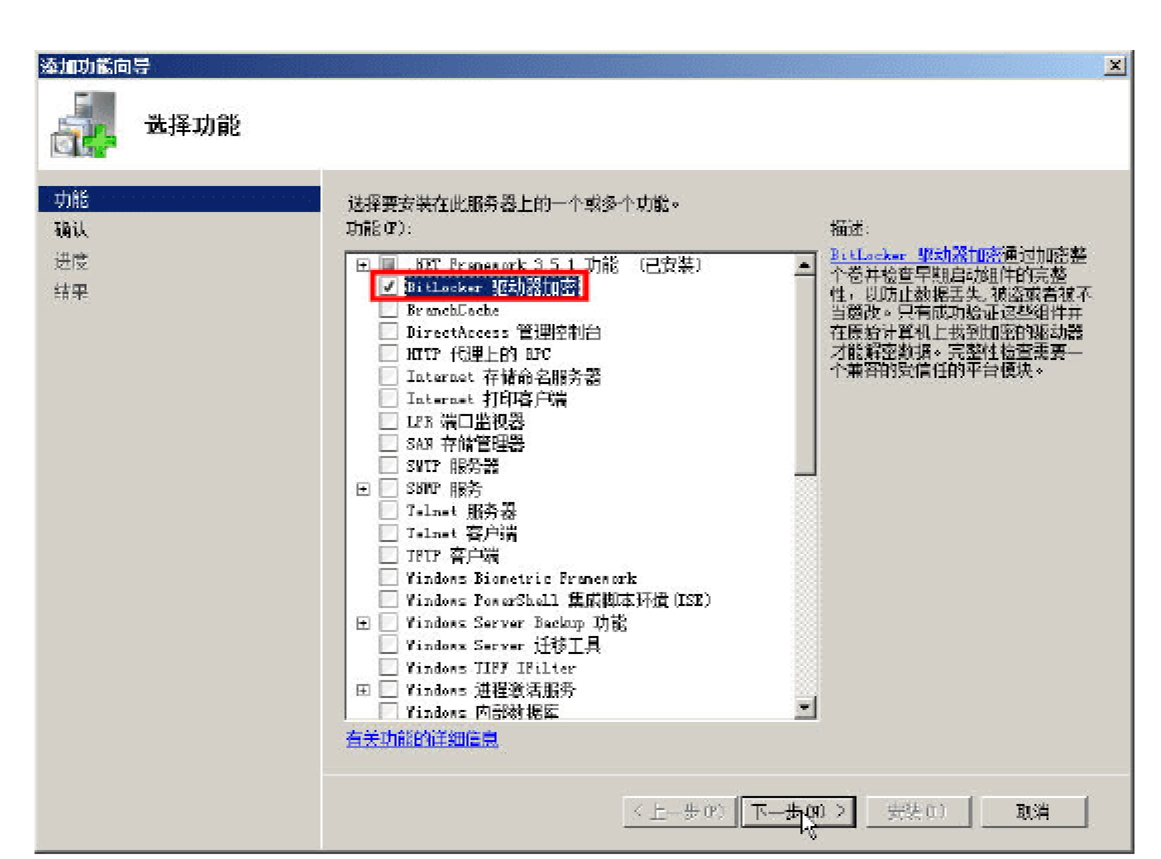


图 4-70　添加 BitLocker 驱动器加密

06 添加 BitLocker 功能后，根据提示，重新启动计算机，如图 4-71 所示。

图 4-71 安装 BitLocker 后重新启动计算机

4.6.4 在 Windows Server 2008 R2 系统卷上启用 BitLocker

添加 BitLocker 驱动器加密功能之后，再次进入 Windows Server 2008 R2，插入 U 盘，为系统卷启用 BitLocker 加密，主要步骤如下。

01 打开“控制面板”，在“查看方式”中选择“小图标”，然后单击“BitLocker 驱动器加密”选项，如图 4-72 所示。

02 打开“BitLocker 驱动器加密”控制面板，在当前列表中，显示了系统中所有的磁盘与分区，从列表中可以看到，当前计算机的磁盘没有启用 BitLocker 驱动器加密功能。如果想对某个磁盘（分区或卷）启用 BitLocker 功能，只要在所选的分区后面单击“启用 BitLocker”链接，并根据提示进行操作既可。在本次操作中，我们将把 C 盘启用 BitLocker 加密，如图 4-73 所示（确认计算机中已经插入 U 盘）。

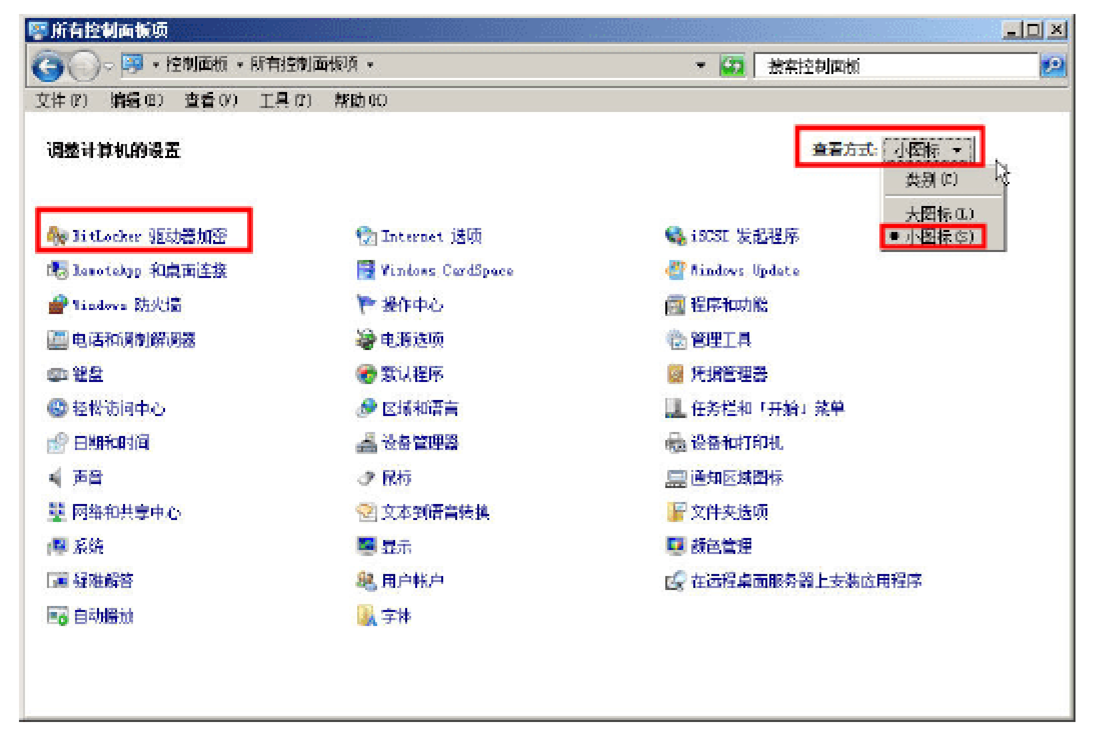


图 4-72 BitLocker 驱动器加密



图 4-73 启用 BitLocker

03 在弹出的“您要启动 BitLocker 安装程序吗？”提示框中，单击“是”按钮，如图 4-74 所示。

04 在“设置 BitLocker 启动首选项”对话框，选择“每次启动时要求启动密钥”选项，如

图 4-75 所示。



图 4-74　启动 BitLocker 安装程序

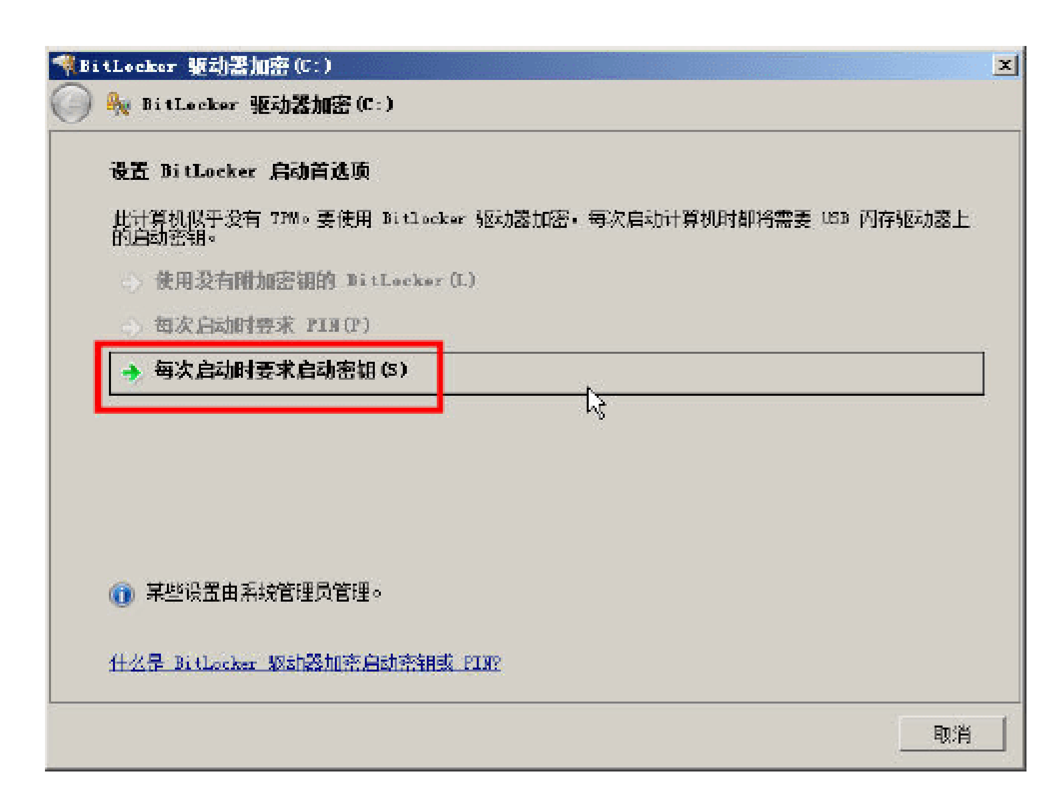


图 4-75　每次启动时要求启动密钥

05 在“保存启动密钥”对话框中，系统列出检测到的 U 盘，如图 4-76 所示。单击“保存”按钮，将启动密钥保存到 U 盘中。

06 在“您希望如何存储恢复密钥”对话框中，根据需要，将恢复密钥保存到 U 盘、文件，或者用打印机直接将恢复密钥打印出来。可根据情况进行选择，如图 4-77 所示。

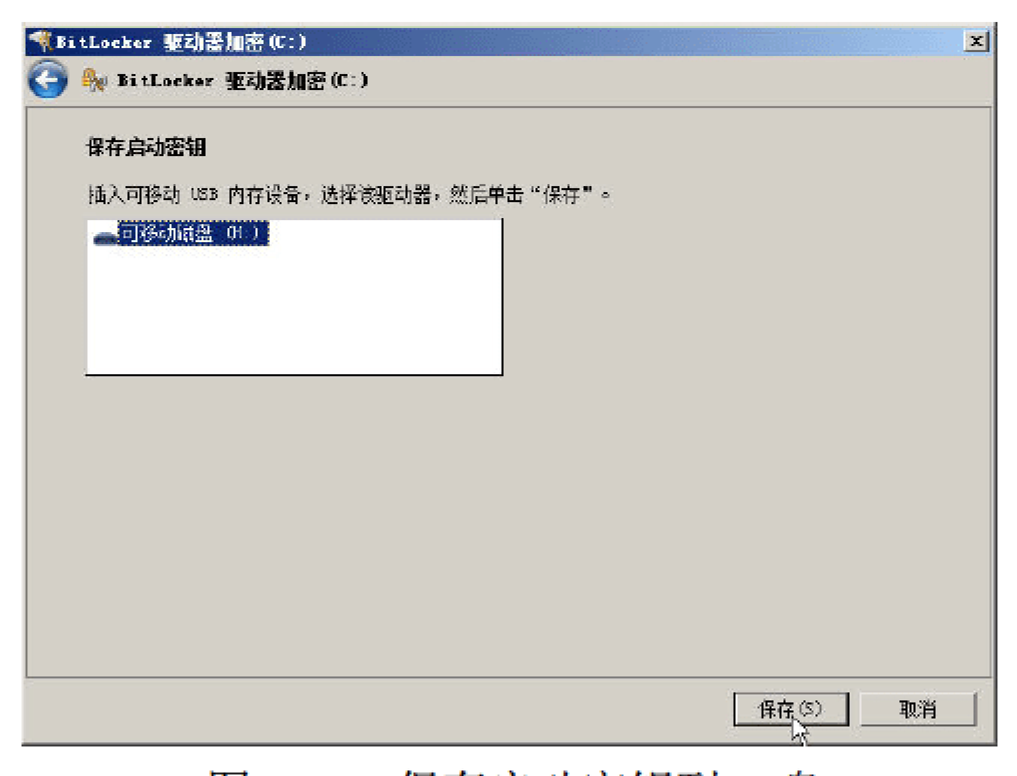


图 4-76　保存启动密钥到 U 盘

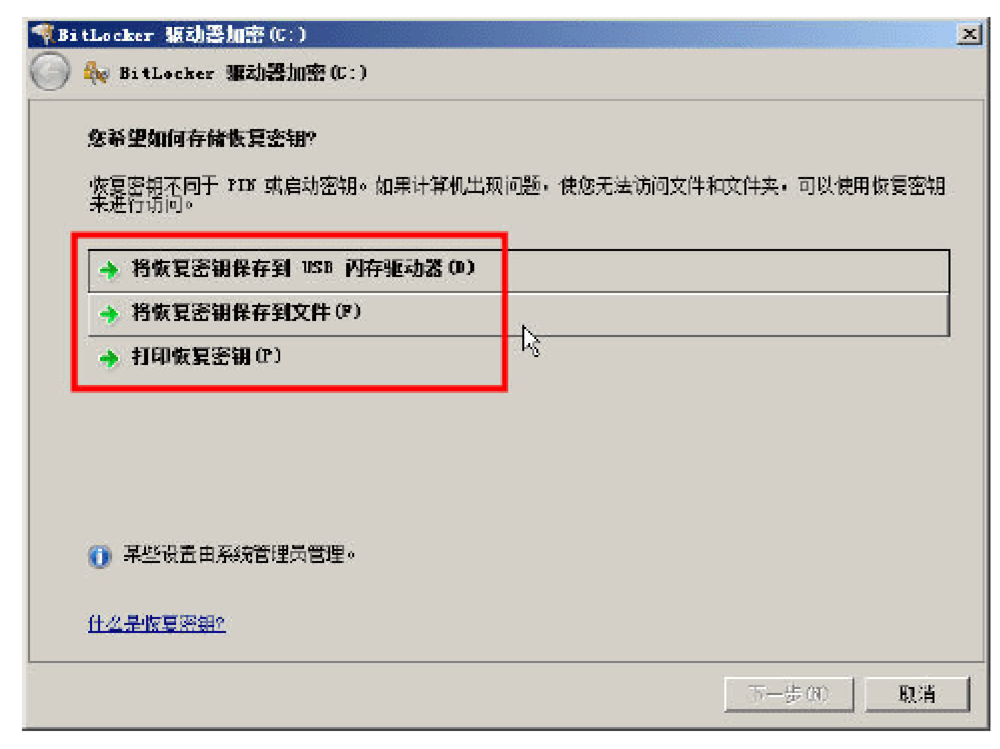


图 4-77　保存恢复密钥

说 明

请将恢复密码保存到安全的位置，最好再将恢复密钥打印并将打印件保存到安全的位置，以后如果保存启动密钥的 U 盘出错、或者计算机的 USB 设备出错，可以用此恢复密钥恢复加密的 BitLocker 驱动器。

07 在“是否准备加密该驱动器”对话框中，选中“运行 BitLocker 系统检查”复选框，然后单击“继续”按钮，如图 4-78 所示。

08 在弹出的“必须重新启动计算机”对话框中，单击“立既重新启动”按钮，重新启动计算机，如图 4-79 所示。

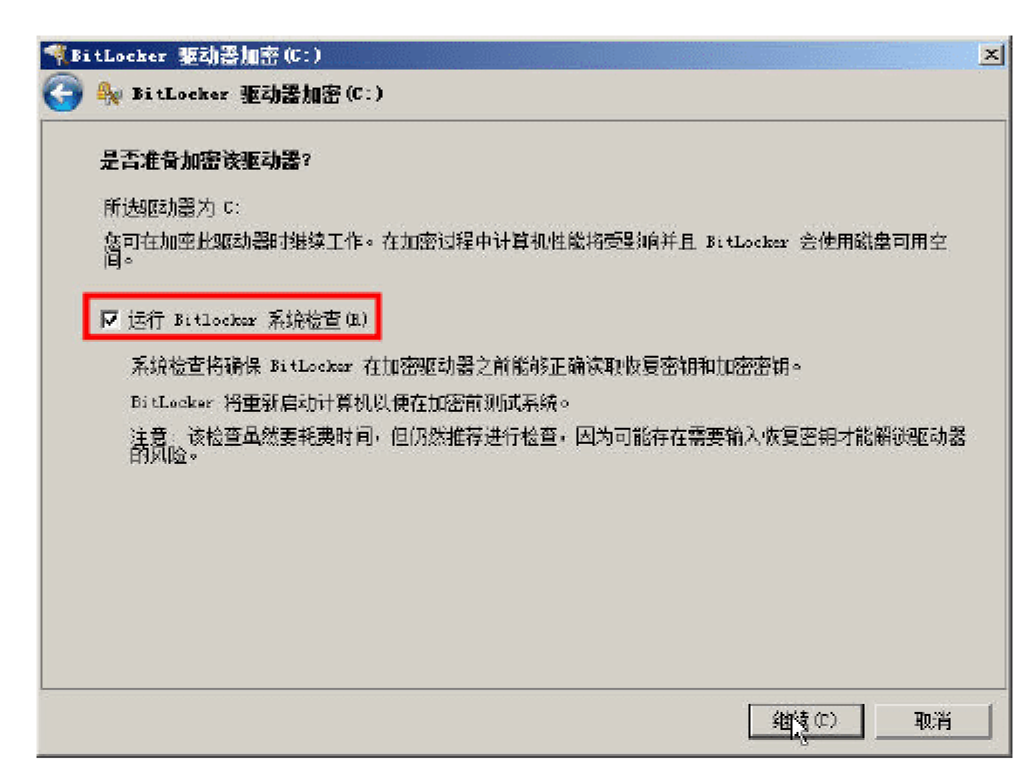




图 4-78　运行 BitLocker 系统检查

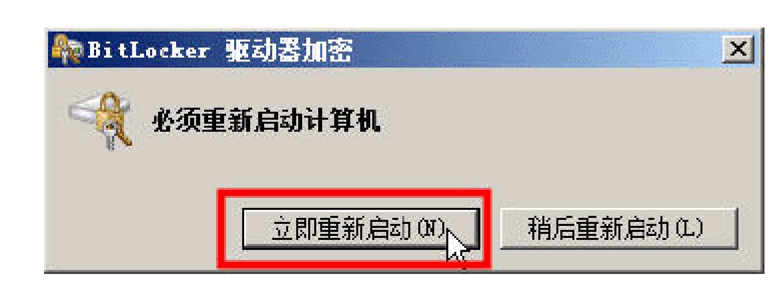


图 4-79　立既重新启动

然后，计算机将重新启动，并在启动的过程中，保持 U 盘不要拔出，当“BitLocker 系统检查”通过并再次进入系统后，将会开始加密系统卷，此时打开“BitLocker 驱动器加密”控制面板，可以看到“加密进行中”的提示，同时启用 BitLocker 加密卷前面出现的“ ”图标，如图 4-80 所示。

此时，双击右下角任务栏上的“ ”图标，会出现“正在加密”的进度提示，如图 4-81 所示。



图 4-80　加密进行中



图 4-81　正在加密系统卷

BitLocker 驱动器加密、解密是需要时间的，以笔者实验的系统为例（4GB 内存、Core E7200、系统卷使用了约 13.5GB），加密大约耗时 50 分钟。

返回到 BitLocker 驱动器加密控制面板，当 BitLocker 驱动器加密完成后，加密后的卷会有三个选项（如图 4-82 所示）：“关闭 BitLocker”（用于关闭 BitLocker 驱动器加密）、“挂起保护”（暂时停用 BitLocker 驱动器加密功能，这在需要更新 BIOS 时使用）、“管理 BitLocker”（用来保存或打印恢复密钥、复制启动密钥等）。

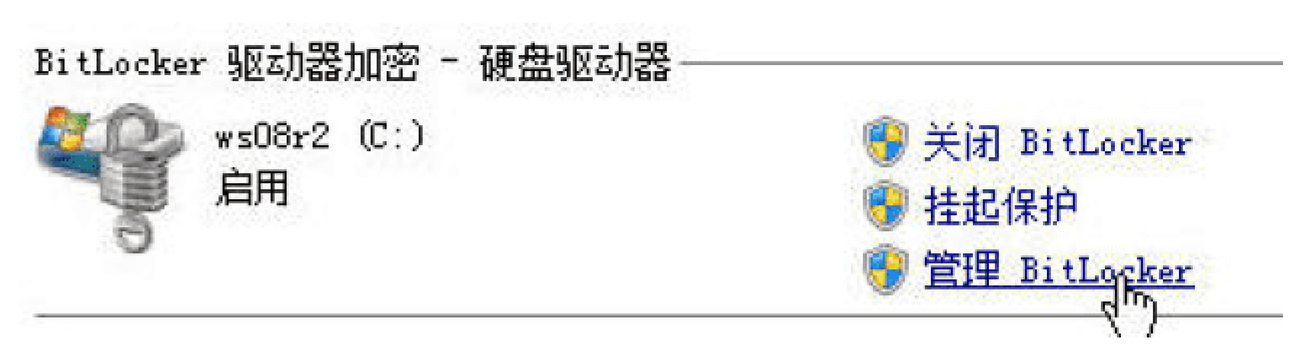


图 4-82　BitLocker 驱动器加密选项

4.6.5　关闭 BitLocker 驱动器加密

BitLocker 恢复密钥是一系列数字，可以用“记事本”打开保存的 BitLocker 恢复密钥（4.6.4 节图 4-77 中保存），记下 BitLocker 恢复密钥，如图 4-83 所示。

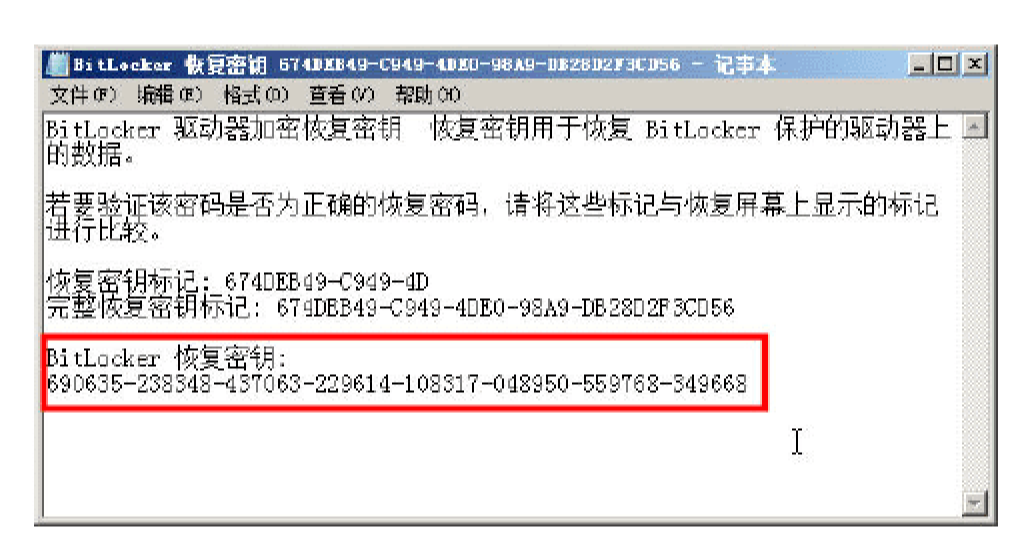


图 4-83　BitLocker 恢复密钥

如果不想再使用 BitLocker 驱动器加密功能，有两种办法：一是拔下加密 U 盘，重新启动计算机后，再提示插入 U 盘，或者解密 BitLocker 驱动器时，按回车键，输入图 4-83 中的“恢复密钥”，即可解密 BitLocker 驱动器。

二是在图 4-82 的 BitLocker 驱动器加密控制面板中，单击“关闭 BitLocker”链接，选择关闭 BitLocker 功能。无论采用何种方式，都可以完成将 BitLocker 驱动器解密的功能。另外，BitLocker 的解密与加密耗费大约相同的时间。

4.6.6　如何使用 BitLocker 驱动器准备工具

在安装 Windows Server 2008 时，如果没有创建 100MB 的“系统保留”分区，将不能启用 BitLocker，此时可以从“http://support.microsoft.com/kb/933246”下载 BitLocker 驱动器准备工具，而不需要重新安装操作系统来启用 BitLocker 功能。BitLocker 驱动器准备工具可自动执行下列过程以正确配置硬盘驱动器。

- 如果有 1 个卷，则创建第 2 个卷，这个卷大约 1.5GB，必须用 NTFS 文件系统格式化。
- 将启动文件移至相应的卷，并确保对操作系统进行了正确的配置，以便以后在启动时可找到这些文件。
- 在驱动器上将相应的卷配置为用于启动的活动分区。

BitLocker 驱动器准备工具完成上述过程后，必须重新启动计算机，这样即可对计算机的硬盘驱动器进行正确配置。此外，还必须初始化或配置受信任的平台模块（TPM）才能启用 BitLocker。

下面将在 Windows Server 2008 的虚拟机中，介绍“BitLocker 驱动器准备工具”的使用。

01 进入“服务器管理器→存储→磁盘管理”中，确认安装 Windows Server 2008 的磁盘只有一个分区，如果有多个分区则删除其余分区，并将第 1 个分区进行扩展，使用整个磁盘，如图 4-84 所示。

02 运行下载的 BitLocker 驱动器准备工具，如图 4-85 所示。

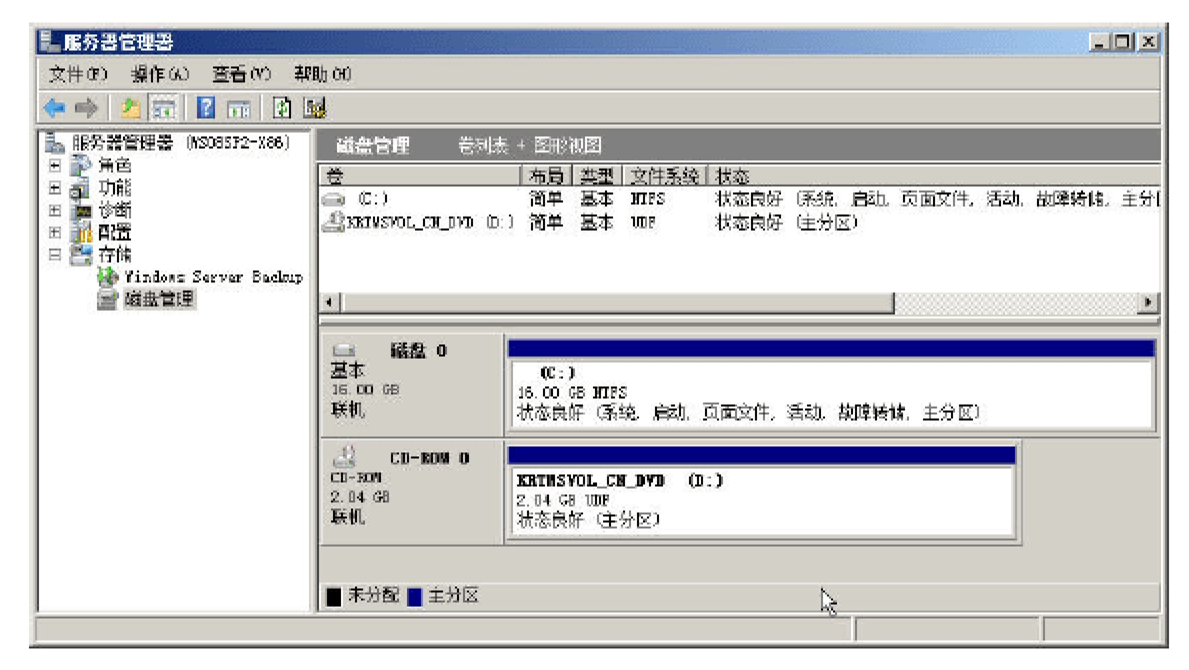


图 4-84　整理磁盘只有一个分区

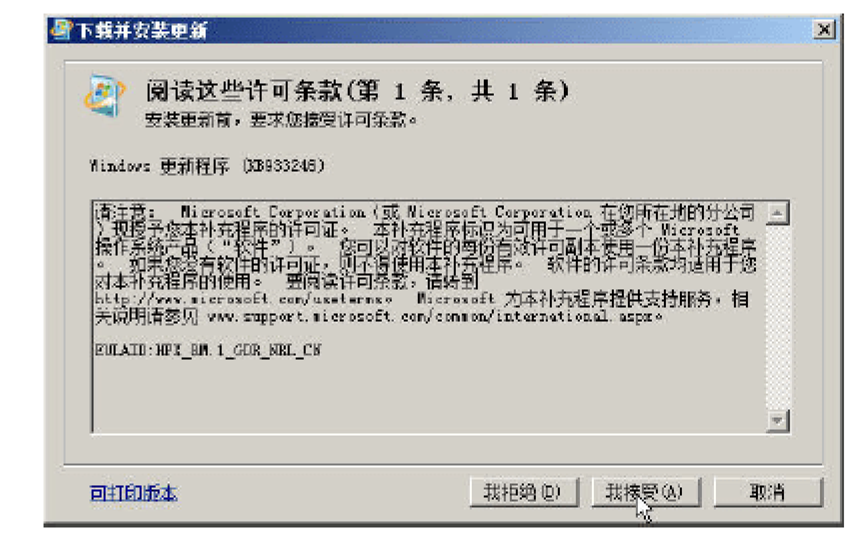


图 4-85　运行 BitLocker 驱动器准备工具

03 安装完成后，从“开始→程序→附件→系统工具→BitLocker”程序组中，选择“BitLocker 驱动器准备工具”，如图 4-86、图 4-87 所示。

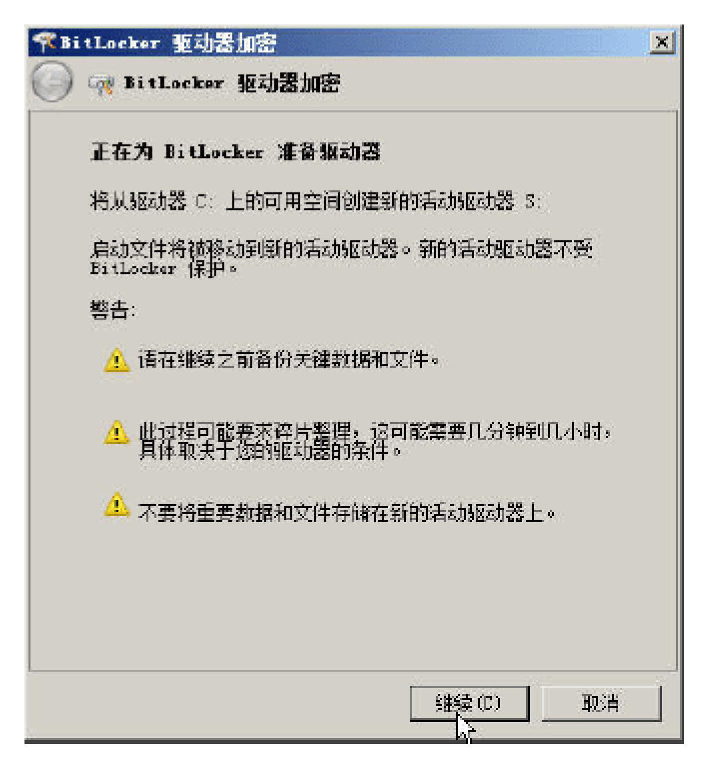


图 4-86　继续

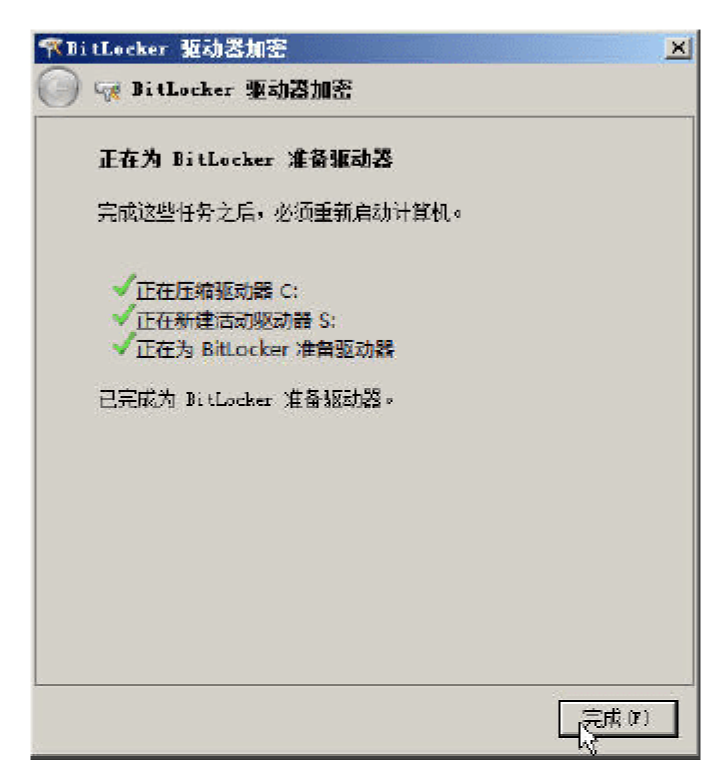


图 4-87　准备驱动器

04 运行 BitLocker 驱动器准备工具之后，重新启动计算机，如图 4-88 所示。

05 再次进入系统后，打开“磁盘管理”，可以看到，当前已经创建了一个盘符为 S、大小为 1.46GB 的主分区，这满足了 BitLocker 驱动器加密的分区要求，如图 4-89 所示。

图 4-88　重新启动计算机

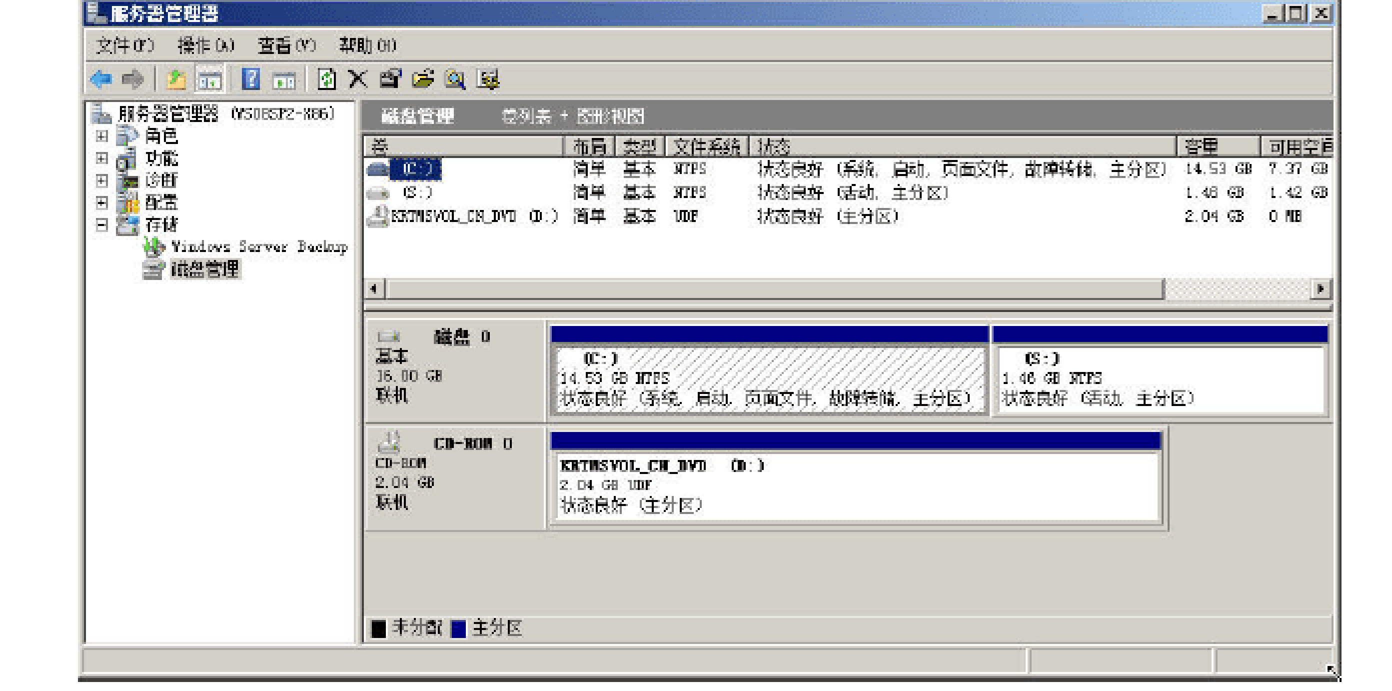


图 4-89　创建分区完成

接下来，就可以参照前文步骤，启用 BitLocker 驱动器加密功能了。

4.7　磁 盘 配 额

在 Windows Server 2008 中，支持“磁盘配额”与“文件夹配额”两种配额方式。磁盘配额是在磁盘分区一级，对不同的用户设置磁盘配额项；而文件夹配额是在文件夹中，对不同的用户分配磁盘配额项。无论是磁盘配额还是文件夹配额，都要求使用 NTFS 文件系统。在默认情况下，磁盘配额与文件夹配额并没有使用，也就是说，允许所有用户无限制的使用磁盘空间，直到空间占满为止。本节介绍启用磁盘配额、创建磁盘配额的方法和步骤。

01 打开“资源管理器”，用鼠标右击要启用磁盘配额的分区，在弹出的快捷菜单中选择“属性”命令，打开磁盘属性对话框。本节以打开 C 分区属性为例进行说明。

02 在“配额”选项卡中，选中“启用配额管理”复选框，如图 4-90 所示。

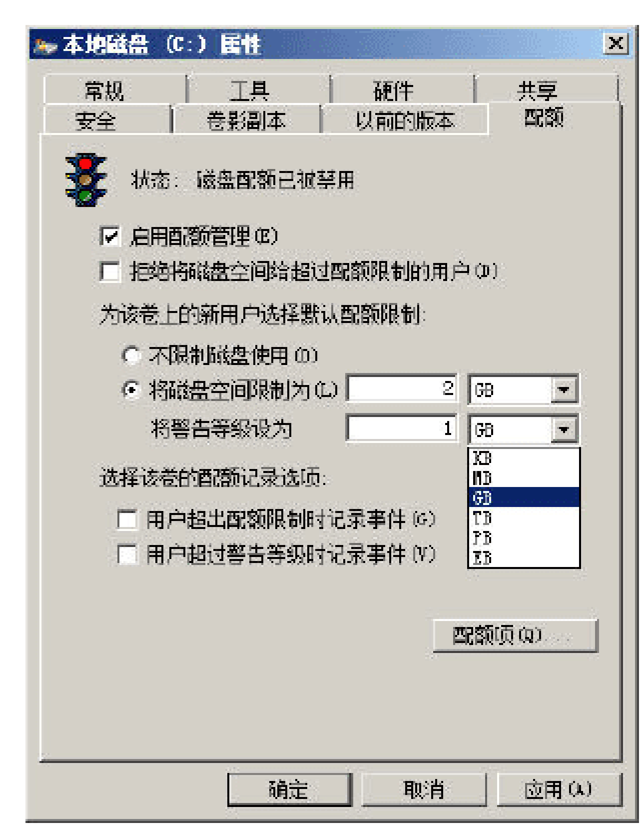


图 4-90　配额管理

如果选中“拒绝将磁盘空间给超过配额项的用户”复选框，那么当用户在此磁盘上使用的空间超过配额项时，就无法再向此磁盘内写任何数据，此时的该磁盘分区属性内，可用空间为 0。如果不选中此项，既使用户在此磁盘上使用的空间超过配额项，仍然可以继续将新的数据保存到此磁盘中。

如果选中“不限制磁盘使用”，则新创建的用户，将可以无限制使用此磁盘空间，如果选中“将磁盘空间限制为”，并且设置限制的大小，例如 2GB，则新建用户（在启用磁盘配额功能后）最大只能使用 2GB。在“将警告等级设为”并且设置大小后，当用户使用的空间达到警告大小时，系统会向用户发出警告提示。

在“选择该卷的配额记录选项”，可以选择是否对用户超出配额项、警告等级时进行记录。

如果要启用配额，可单击“应用”按钮，为图 4-90 的设置启用配额。

03 如果要对系统已有的用户创建新的配额项，须在图 4-90 中，单击“配额项”按钮，打开配额项管理对话框，如图 4-91 所示。

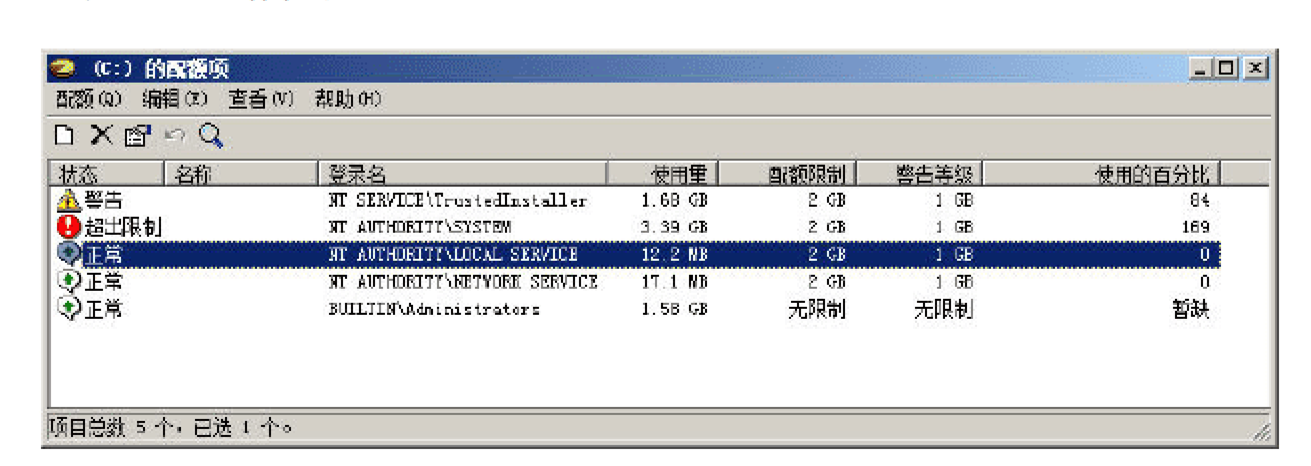


图 4-91　配额项

04 在图 4-91 中，单击“配额”菜单，选择“新建配额项”命令，在弹出的“选择用户”对话框中，选择要进行磁盘配额的用户，例如 ws01，将弹出“添加新配额项”对话框，在此对话框中，为选中的用户选择限制空间及警告空间，如图 4-92 所示。

05 在创建配额项后，也可以删除创建的配额项，如图 4-93 所示。

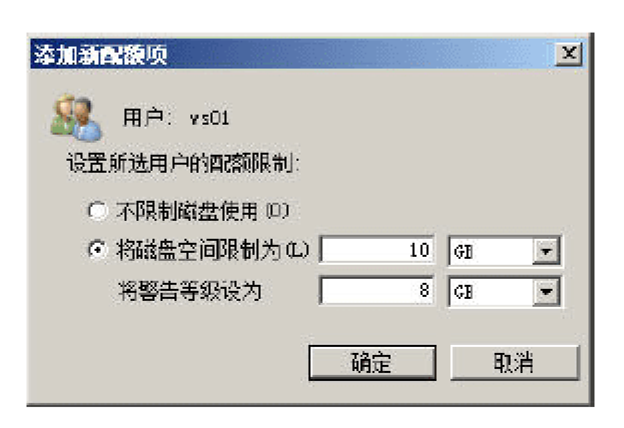


图 4-92　新建配额项

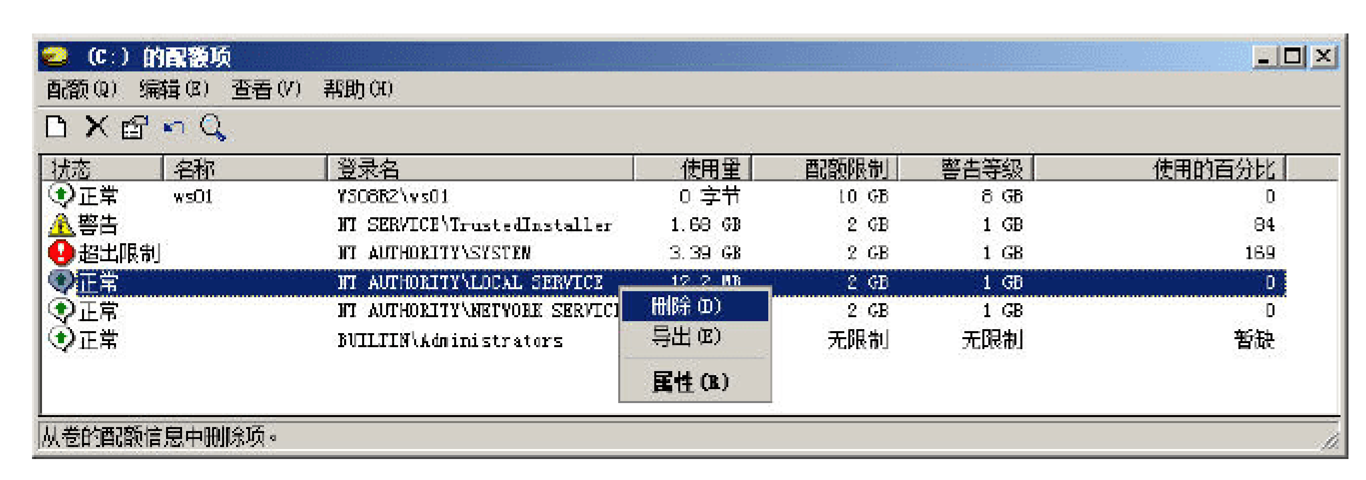


图 4-93　删除配额项

06 如果要关闭磁盘配额，可以在“配额”选项卡中，取消选中“启用配额管理”复选框，并单击“确定”按钮，既可关闭配额，如图 4-94 所示。

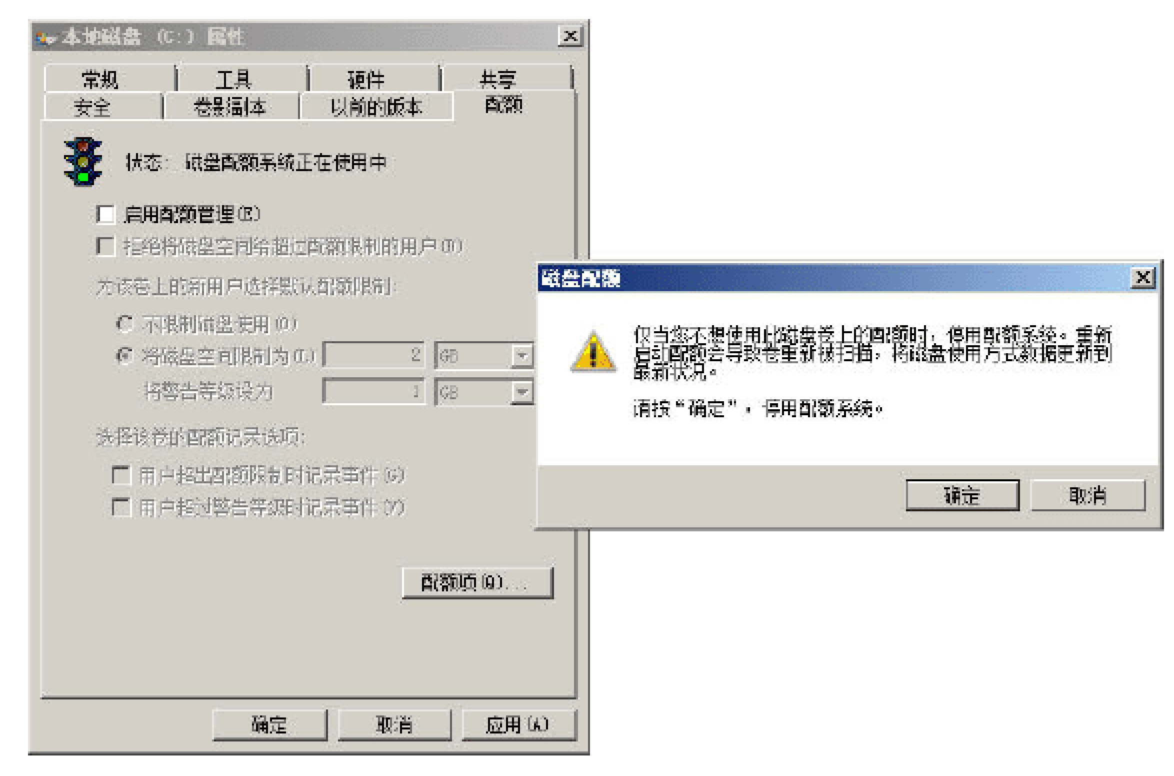


图 4-94　关闭磁盘配额

4.8　文件夹配额与文件屏蔽

磁盘配额，只能对整个分区进行配置。如果用户需要有不同的配额，只能在规划磁盘分区时，创建多个分区，并且在不同的分区为用户创建不同的配额。并且，分配给用户的配额并不能区分用户是用来保存数据，还是保存电影、音乐等。从 Windows Server 2003 R2 开始，Windows Server 引入了“文件夹配额”与“文件屏蔽”功能，以满足管理员对文件系统、文件空间更进一步管理的需求。使用“文件夹配额”，管理员可以在同一个分区，在不同的文件夹中，对用户进行不同的配额。而使用“文件屏蔽”功能，可以限制用户保存在文件夹中的文件类型是管理员所允许的类型，例如，只允许用户保存文档而不能保存 MP3 文件等。

4.8.1　添加文件服务器资源管理器

在本小节中，将介绍如何添加文件服务器资源管理器，步骤如下。

01 进入“服务器管理器”，添加角色，在“选择服务器角色”对话框中，选中“文件服务”复选框，如图 4-95 所示。

02 在“选择角色服务”对话框中，选中“文件服务器资源管理器”复选框，如图 4-96 所示。



图 4-95　添加文件服务

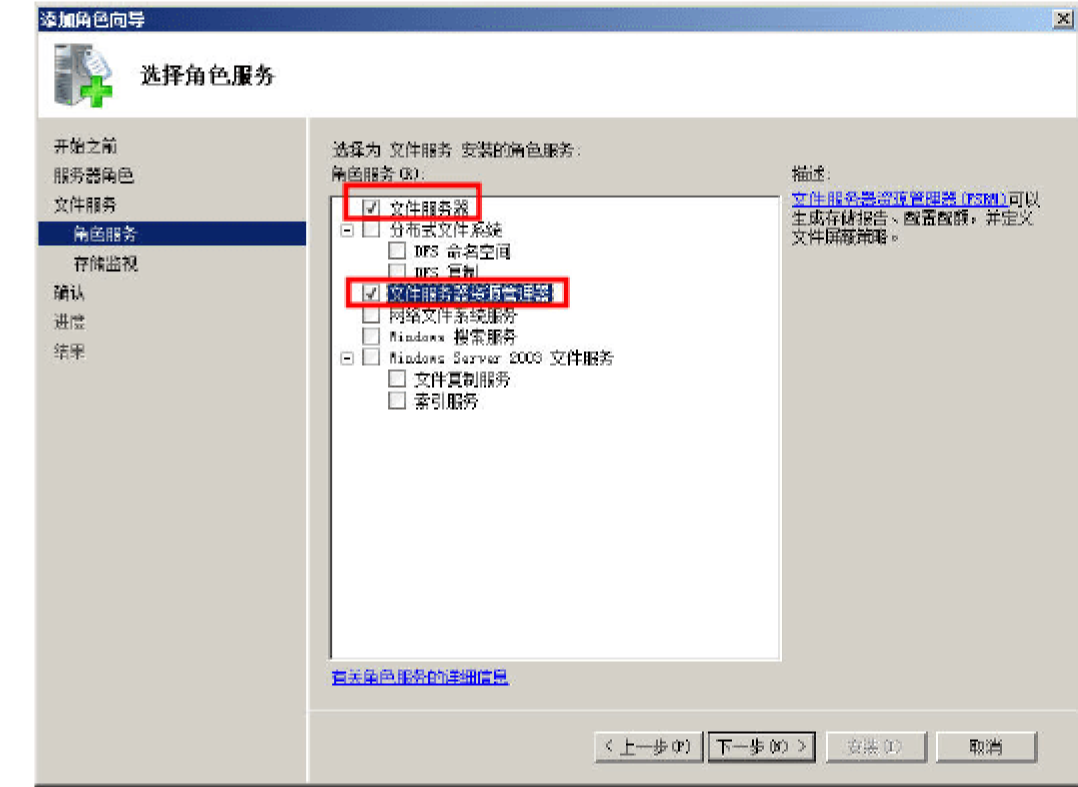


图 4-96　文件服务器资源管理器

03 在“配置存储使用情况监视”对话框中，选择 C 分区，如图 4-97 所示。

04 在“设置报告选项”对话框，选择默认值，如图 4-98 所示。

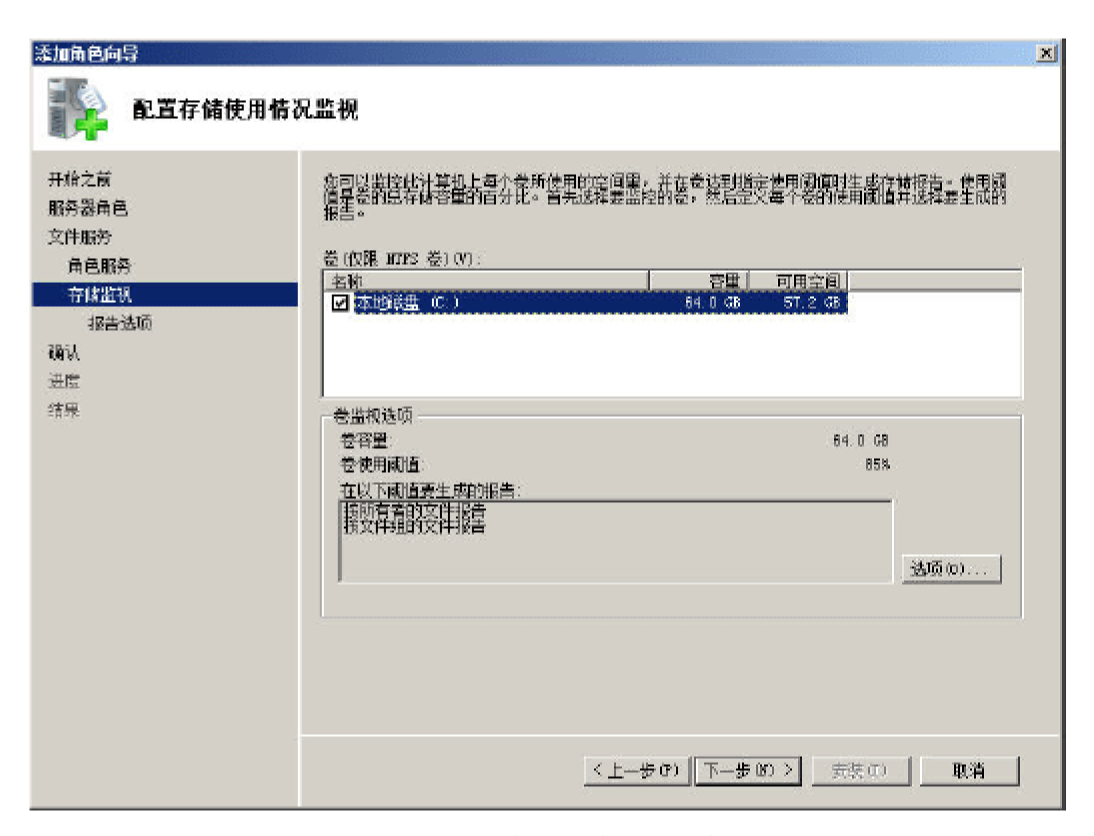


图 4-97　配置存储使用情况监视

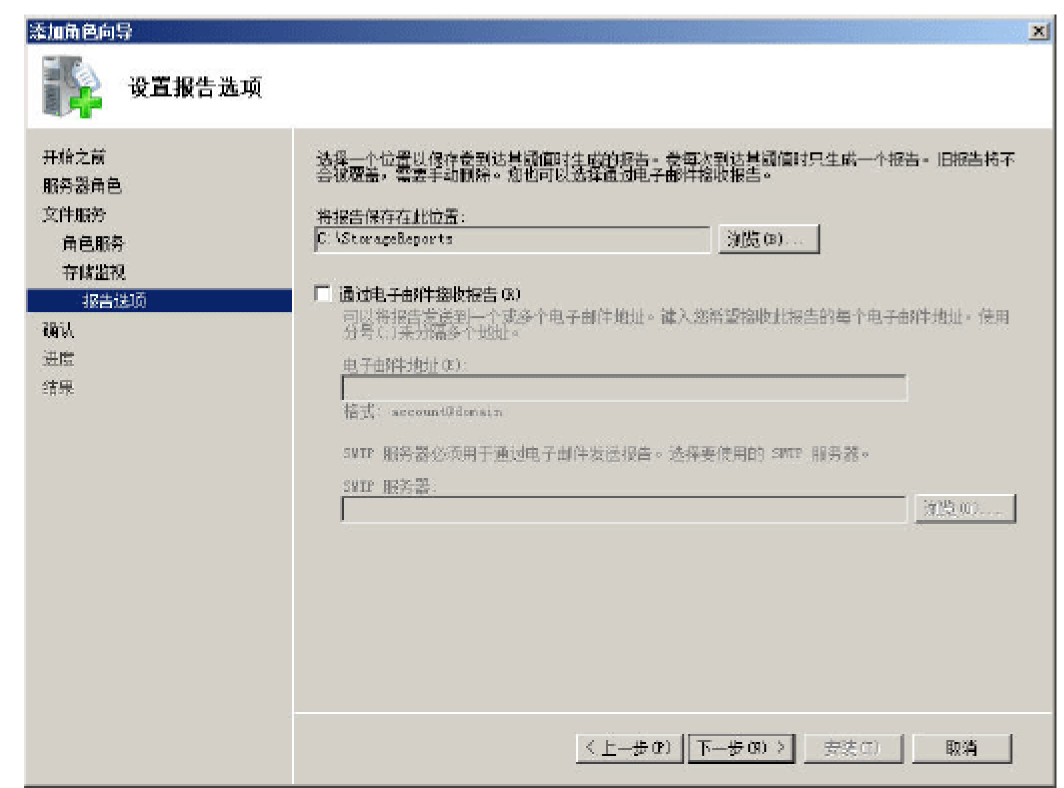


图 4-98　设置报告选项

05 在“确认安装选择”对话框，单击“安装”按钮，开始安装文件服务器资源管理器。安装完成之后，单击“关闭”按钮，如图 4-99 所示。



图 4-99　安装完成

4.8.2　创建文件夹配额

本小节在 C 盘创建一个 File1 的文件夹，在该文件夹创建文件夹配额，步骤如下。

01 在“服务器管理器”对话框中，定位到“角色→文件服务→共享和存储管理→文件服务器资源管理器→配额管理→配额”，在右侧的窗格中用鼠标右击，在弹出的快捷菜单中选择“创建配额”命令，如图 4-100 所示。

02 在“创建配额”对话框中，在“配额路径”选项组中，单击“浏览”按钮，浏览选择要启用文件夹配额的目录，在本例中为 C:\File1，然后选中“在现有子文件夹和新的子文件夹中自动应用模板并创建配额”复选框，在“从此配额模板派生属性”下拉列表中，选择适合的配额，如图 4-101 所示。如果列表中的配额不适用，可以单击“定义自定义配额属性”并单击“自定义属性”对话框，设置自定义的配额。

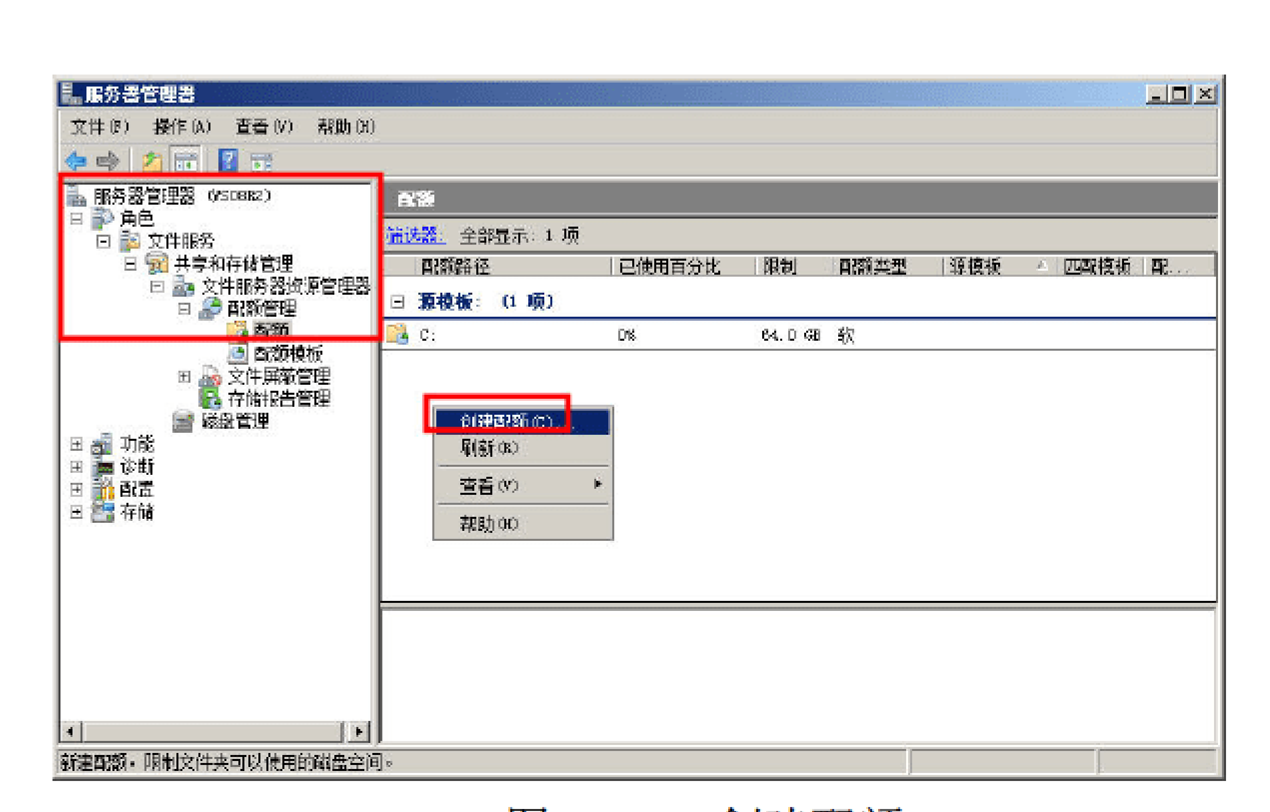



图 4-100　创建配额

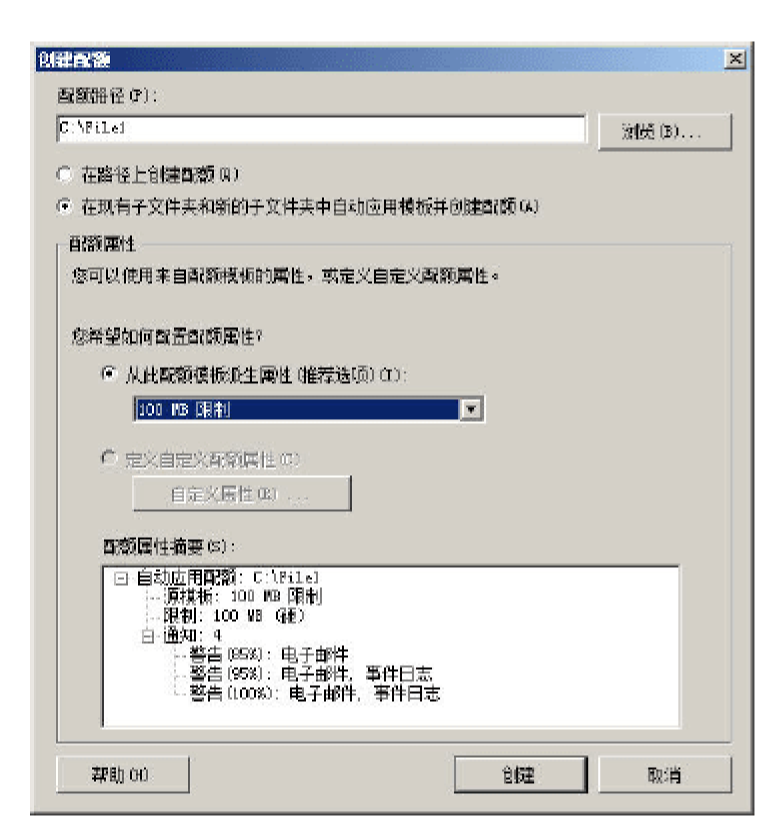


图 4-101　选择配额

03 选择配额模板之后，单击“创建”按钮，创建文件夹配额。

04 在“配额管理→配额模板”中，列出了系统自定义的模板，如图 4-102 所示。可以双击某个模板进行修改，也可以在此创建新的模板。

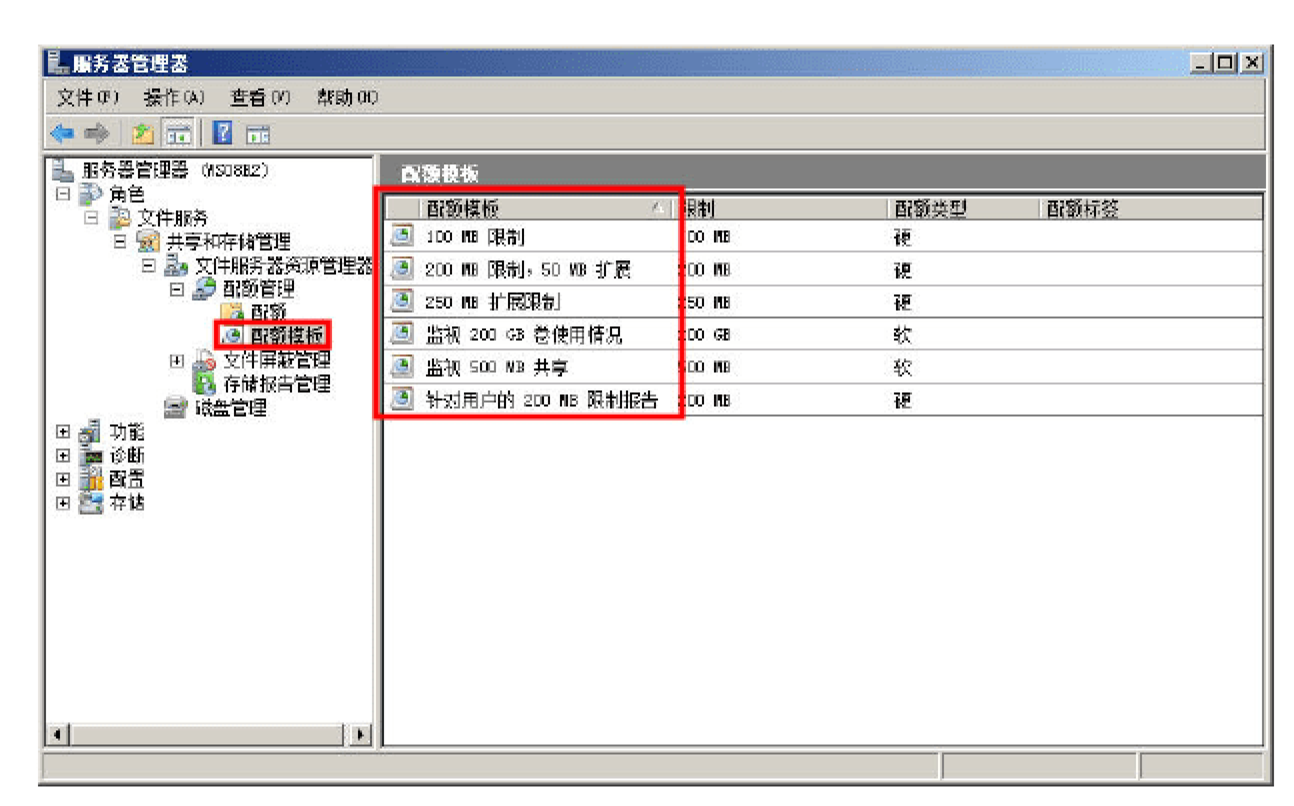


图 4-102　配额模板

4.8.3　创建文件屏蔽

本小节介绍创建文件屏蔽的操作，步骤如下。

01 定位到“文件服务器资源管理器→文件屏蔽管理→文件屏蔽”，在右侧的空白窗格中右击，在弹出的快捷菜单中，选择“创建文件屏蔽”命令，如图 4-103 所示。

02 在弹出的“创建文件屏蔽”对话框中，在“文件屏蔽路径”中选择 C:\File1 文件夹，表示将在该文件夹启用文件屏蔽。然后在“从此文件屏蔽模板派生属性”下拉列表中，选择要屏蔽的文件类型，如图 4-104 所示。在本例中选择“阻止音频文件和视频文件”。

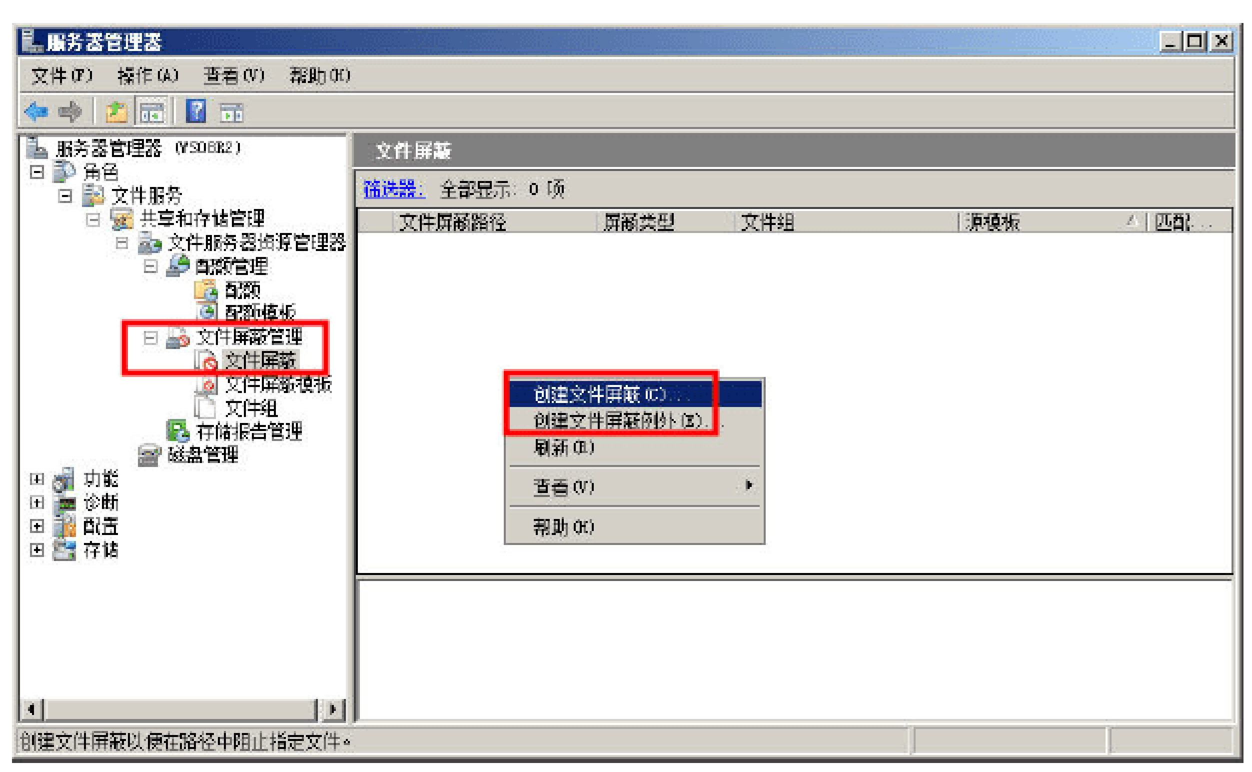


图 4-103　创建文件屏蔽

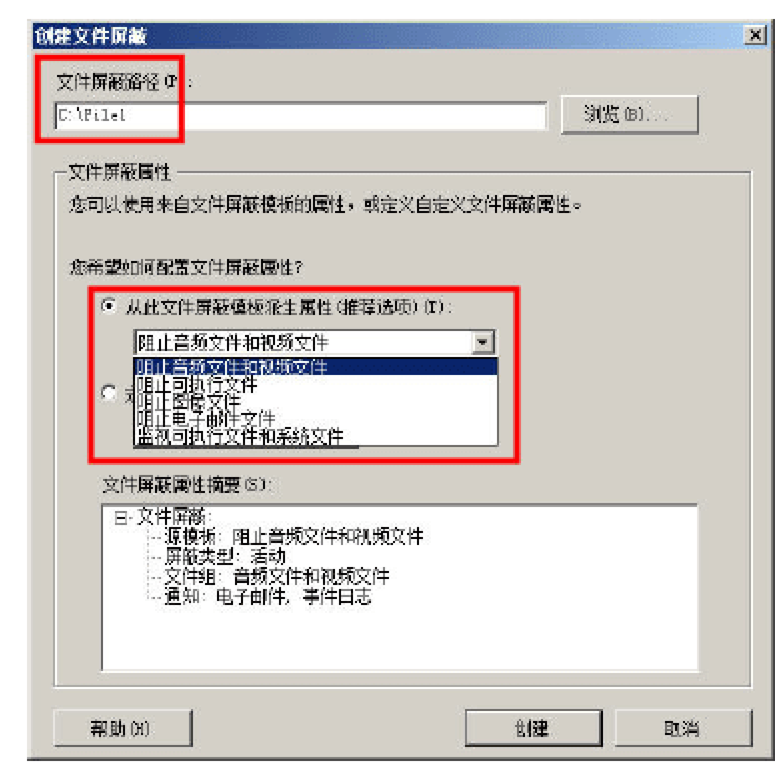


图 4-104　选择文件屏蔽类型

03 创建文件屏蔽后，将阻止指定类型的文档保存在启用文件屏蔽的目录中。

04 还可以创建“文件屏蔽例外”，保存用户指定的文档。在图 4-103 中，选择“创建文件屏蔽例外”，将打开“创建文件屏蔽例外”对话框，在“例外路径”中，选择 C:\File1，然后在“文件组”列表中，选择从屏蔽中排除的文件组，以保存指定的文件，如图 4-105 所示。在本例中选择了“Office 文件”、“电子邮件文件”、“图像文件”、“文本文件”、“压缩文件”等。

05 创建文件屏蔽后如图 4-106 所示。

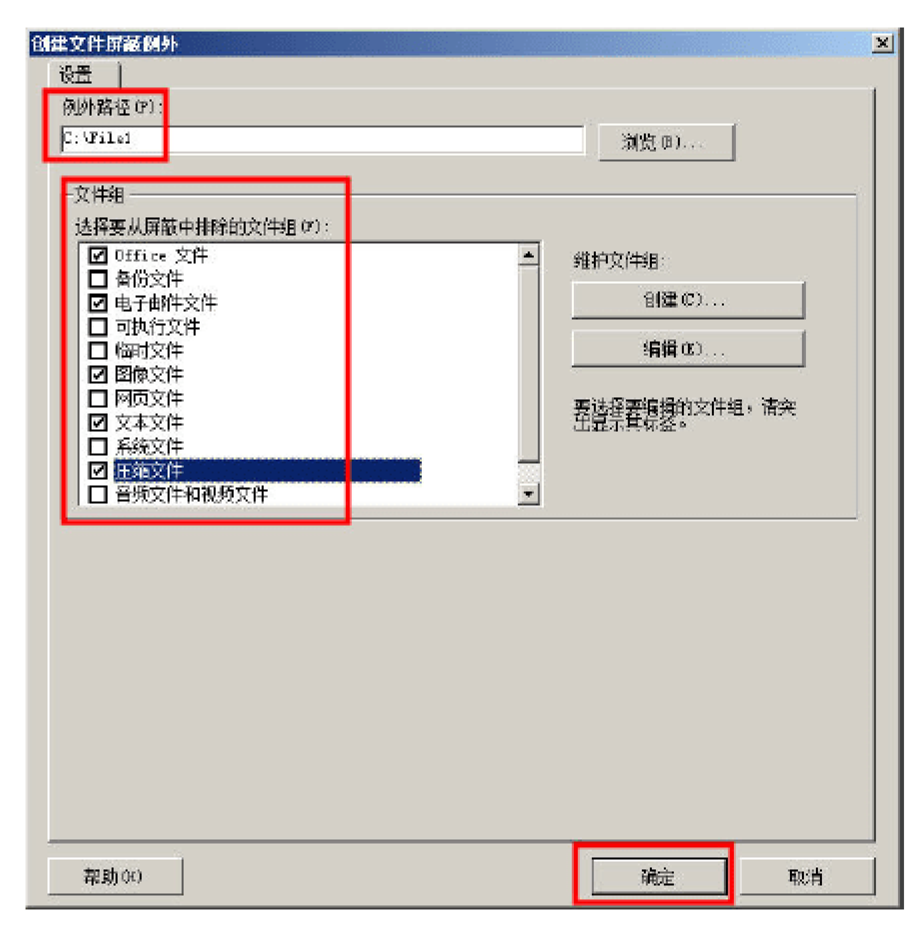


图 4-105　创建文件屏蔽例外

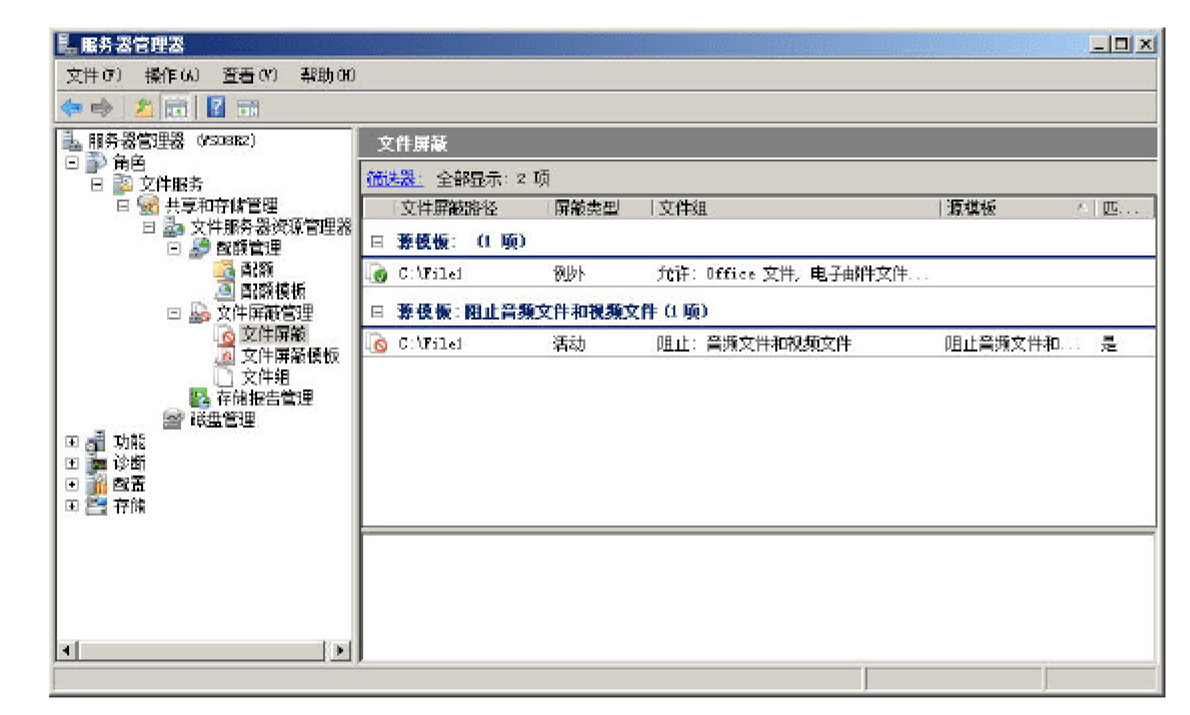


图 4-106　文件屏蔽

也可以在图 4-106 中，选中创建的文件屏蔽或文件屏蔽例外进行删除。或者在“文件屏蔽管理器→文件屏蔽模板”中管理或添加、删除模板。

4.8.4　测试文件夹配额与文件屏蔽

打开“资源管理器”，测试文件夹配额与文件屏蔽，步骤如下。

01 打开 C:\File1 文件夹，向其中拷贝文本文件或图像文件（或者创建扩展名为 bmp 或 txt 的文件），拷贝成功，如图 4-107 所示。

02 向文件中拷贝音频或视频文件，出现错误，如图 4-108 所示。

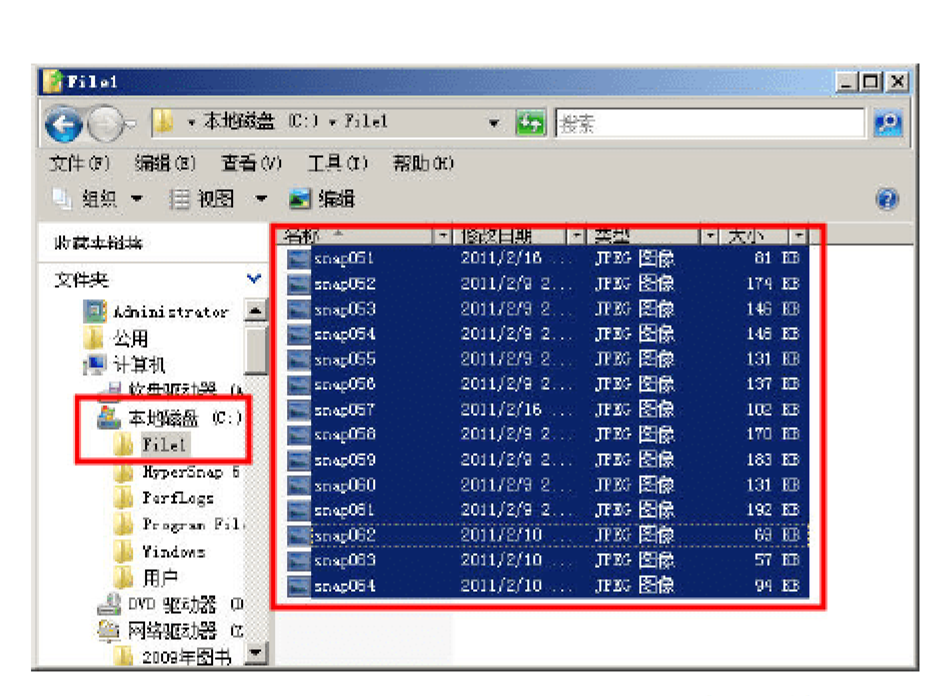


图 4-107　拷贝或创建图像文件

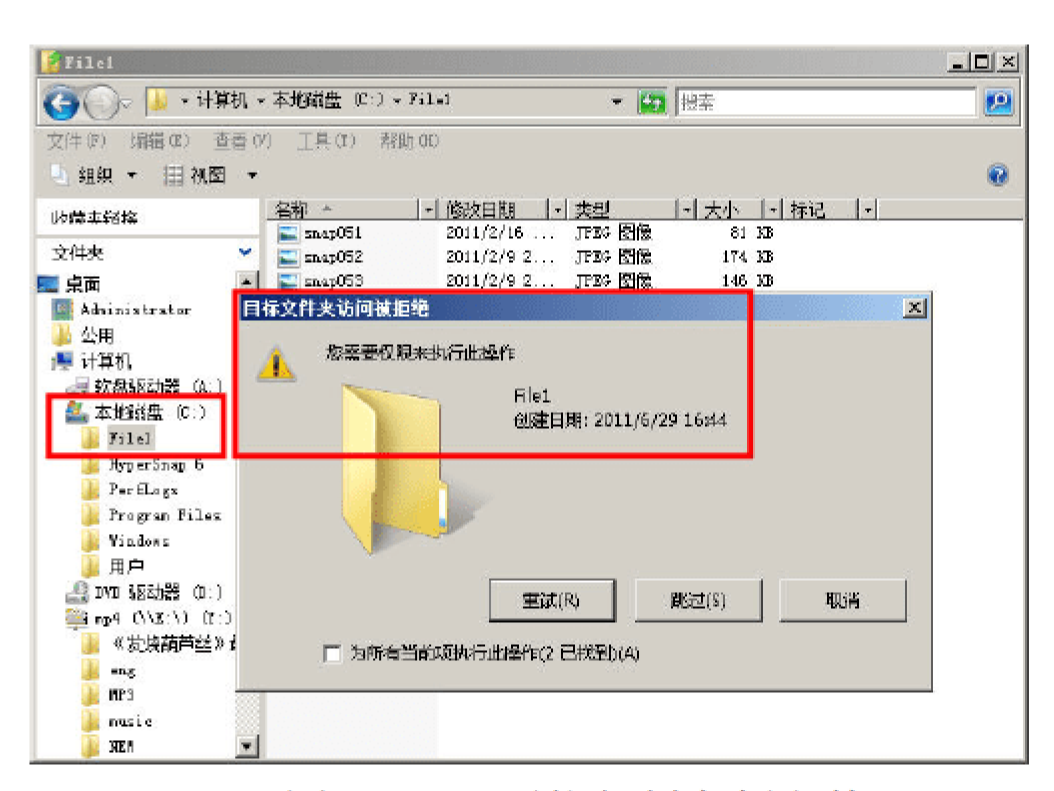


图 4-108　不能复制音频文件

03 拷贝其他文件，当复制的文件超过 100MB 时，出现“磁盘空间不足”错误提示，如图 4-109 所示。

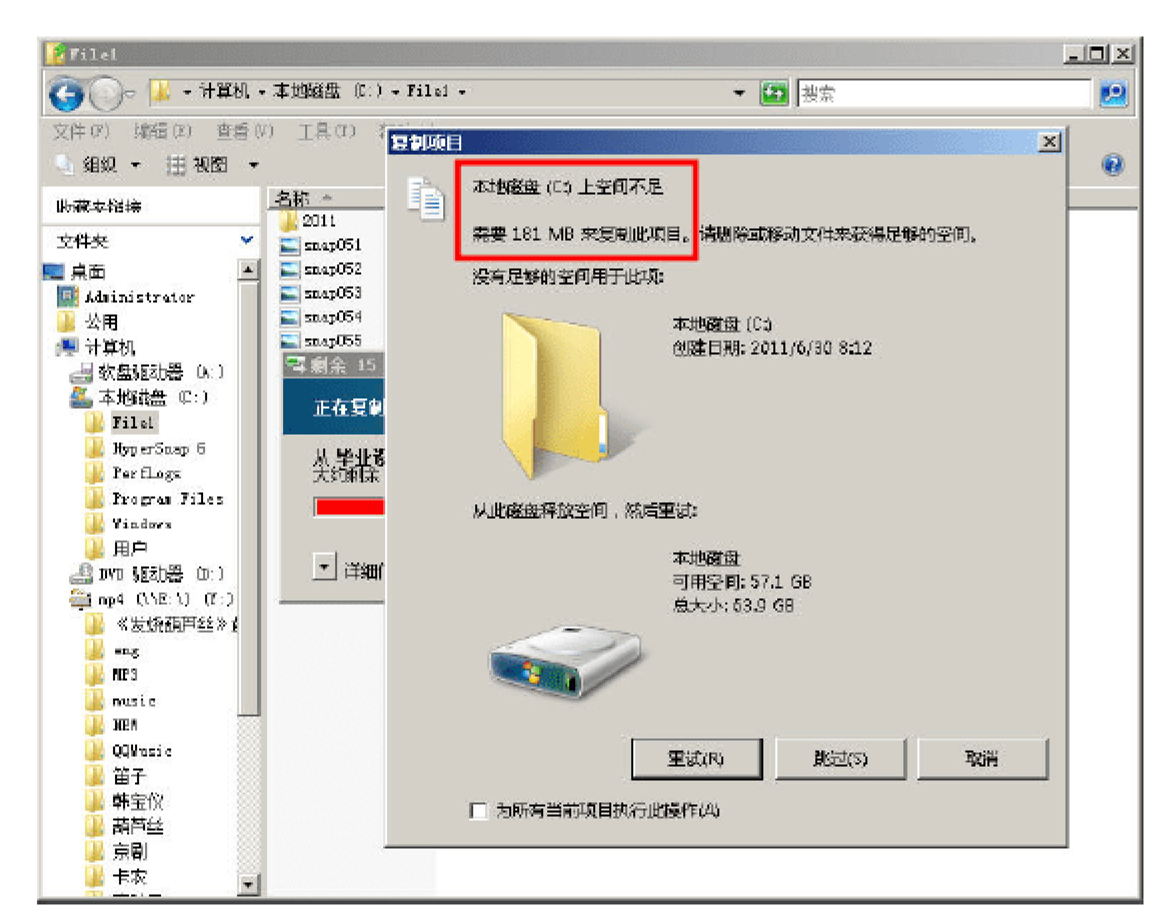


图 4-109　提示磁盘空间不足

4.9　文件和打印机共享

在不同的计算机之间，如果有“文件”或“文件夹”等数据需要交换或拷贝，通常有以下几

种方式：

（1）使用可移动介质。可以将文件复制到任何可移动介质中，包括 U 盘、移动硬盘、CD、DVD 和闪存卡。然后可以将该介质插到另一台计算机上，将文件复制到该计算机中，或将该可移动介质交给要共享文件的人，让他们自己复制文件。

（2）通过电子邮件。如果只需要共享一两个文件，且文件不大，那么最简单的方式便是将其附加到电子邮件中实现共享。

（3）网站或 FTP 服务器。通过网站的“网络共享”或 FTP 服务器实现共享。

（4）使用既时消息软件。大多数即时消息软件允许用户在与其他人联机聊天时共享文件，例如 QQ 与 MSN，都可以在聊天的双方之间传送文件（QQ 还可以传送文件夹）。

（5）共享文件夹。对于局域网来说，使用“共享文件夹”是最简单、也是最方便的方式。

4.9.1　共享文件夹与共享权限

本节将介绍共享文件夹的使用。

使用“共享文件夹”，可以让局域网中的其他计算机，通过“共享文件夹”访问服务器端提供的资源。在使用“共享文件夹”的时候，服务器与客户端只是相对的，凡是提供“共享文件夹”服务的，都可以称作“服务器端”，例如，在某些时间，如果一台 Windows XP 的工作站创建并提供共享文件夹服务，且一台 Windows Server 2008 需要访问并使用这台 Windows XP 提供的共享文件夹，则此时 Windows XP 可以称作“服务器端”，而 Windows Server 2008 则可以称作“客户端”。

网络服务或网络应用的目的，是让指定的用户、在指定的时间、以指定的行为或指定的权限、访问指定的资源。共享文件夹也不例外，为了让网络中的客户端安全、可靠的访问或使用服务器端提供的共享资源，必须对“共享文件夹”做出权限设置。通常来说，共享权限包括“读取”、“更改”与“完全控制”几种。

共享文件夹提供了一个“访问接入点”，当用户使用“共享文件夹”访问服务器提供的资源时，除了受“共享权限”限制外，还与服务器端所共享的文件夹的“NTFS”权限限制有关。“共享文件夹”只是一个“相对”的权限，而“NTFS 权限”则是一个“绝对”的权限。例如，在服务器上，E 盘有个 abcd 的文件夹，设置了两个共享，共享名分别为 aaaa 与 bbbb，如果 aaaa 与 bbbb 的共享权限不同，则用户通过 aaaa 与 bbbb 共享文件名访问服务器 E 盘的 abcd 文件夹时，其权限也是不同的。

当通过共享文件夹访问服务器提供的资源时，用户的权限是所使用的共享文件夹权限与文件夹本身的 NTFS 权限的“交集”，例如，abcd 文件夹的权限是对所有用户“读取与更改”，而 aaaa 的权限是对所有用户“读取”、bbbb 的权限是对所有用户有“更改”权限，则用户通过 aaaa 访问时，用户的有效权限是“读取”，而通过 bbbb 共享点访问时，用户的有效权限是“更改”。

4.9.2　创建共享文件夹

下面通过一个具体的实例，介绍在服务器的 E 盘创建一个名为 software 的文件夹，并将其创建为共享文件夹，设置共享权限的方法，主要步骤如下。

01 关闭 Windows 2008 的虚拟机，并向虚拟机中再次添加一个 100GB 左右的虚拟硬盘，然

后打开 Windows 2008 虚拟机，进入系统后，在“计算机管理→存储→磁盘管理”中，为新建的硬盘创建两个分区，盘符分别为 E 和 F，如图 4-110 所示。

02 打开“资源管理器”，定位到 E 盘，在 E 盘创建一个名为 software 的文件夹，用鼠标右击，在弹出的快捷菜单中选择“共享”命令，如图 4-111 所示。

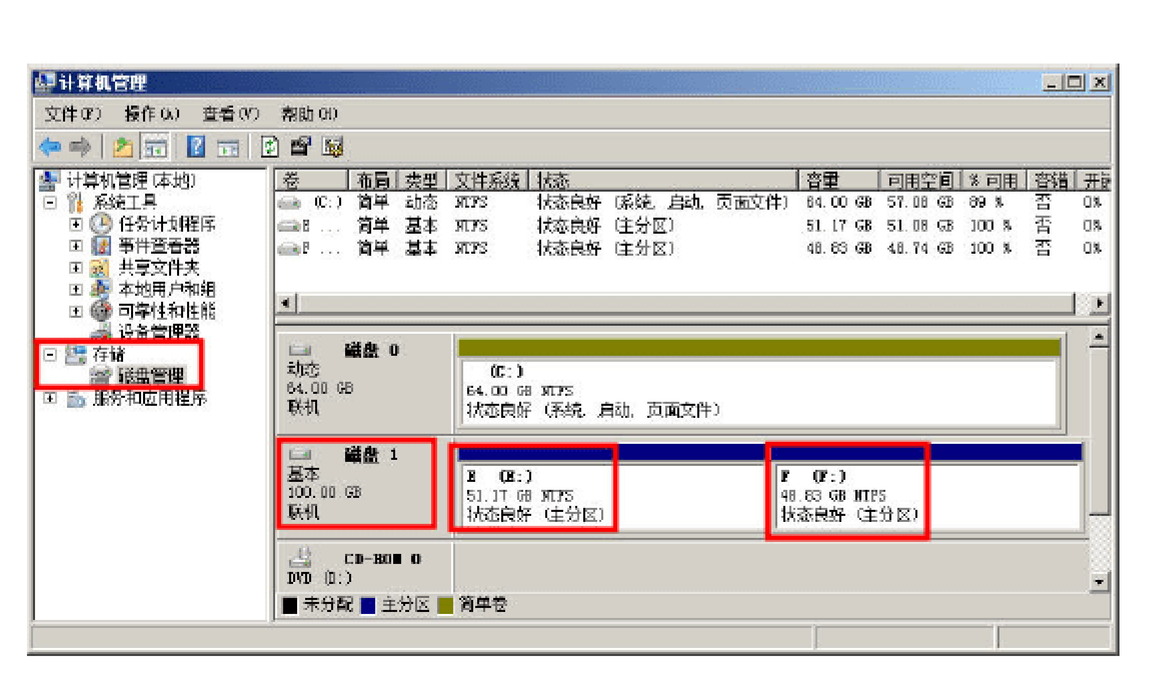


图 4-110　添加硬盘并创建两个分区

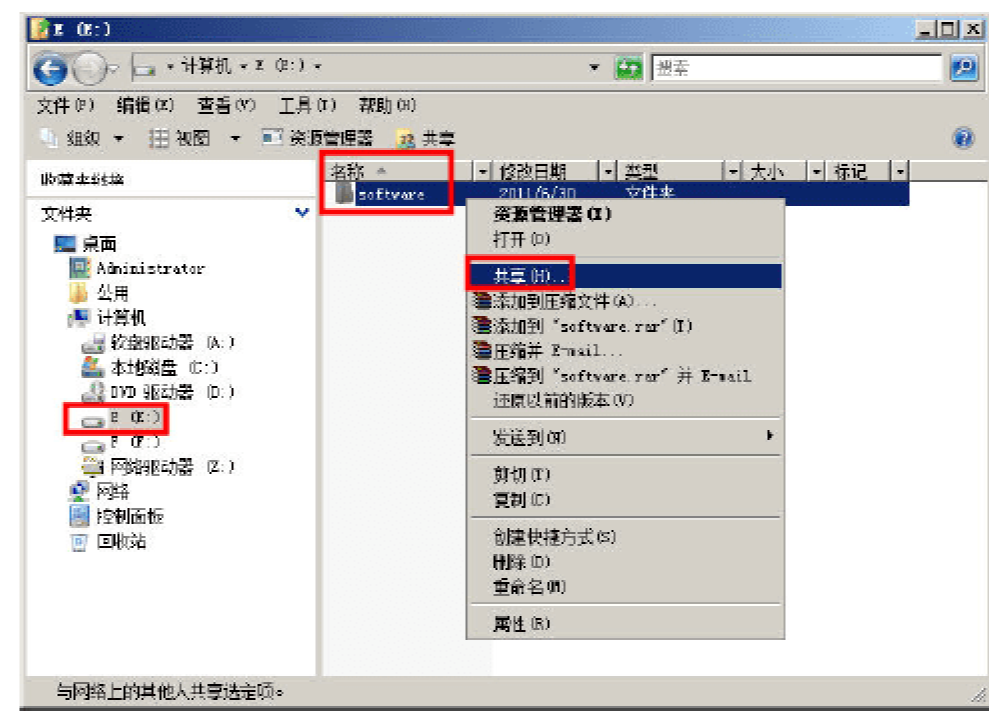


图 4-111　共享

03 在弹出的“文件共享”对话框中，单击“添加”按钮前面的“▼”下拉按钮，在弹出的下拉列表中，选择要与其共享的用户或用户组，如图 4-112 所示。在本例中，选择“Everyone”用户组，该用户组代表所有用户。

04 在选择要添加的用户或组后，单击“添加”按钮，将其添加到列表中，然后在添加的用户（或组）一行中，在“权限级别”列表中，单击“▼”下拉按钮，在弹出的权限中，选择要分配的权限，这可以从“读者—读取权限”、“参与者”、“共有者”之间选择，如图 4-113 所示。设置之后，单击“共享”按钮。

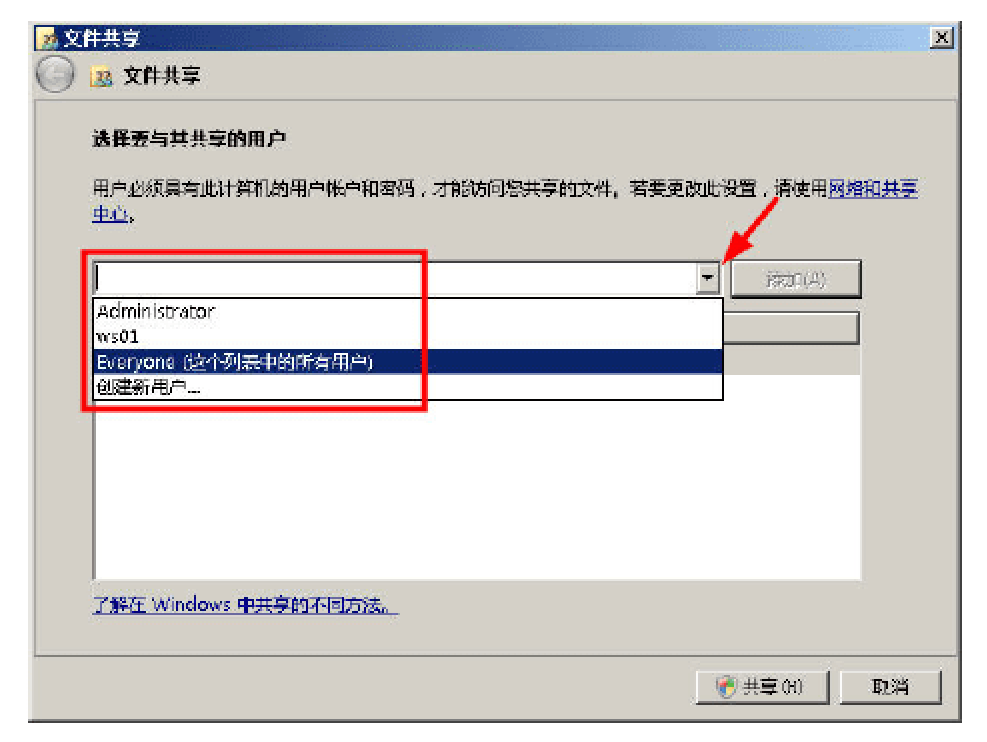


图 4-112　选择用户组

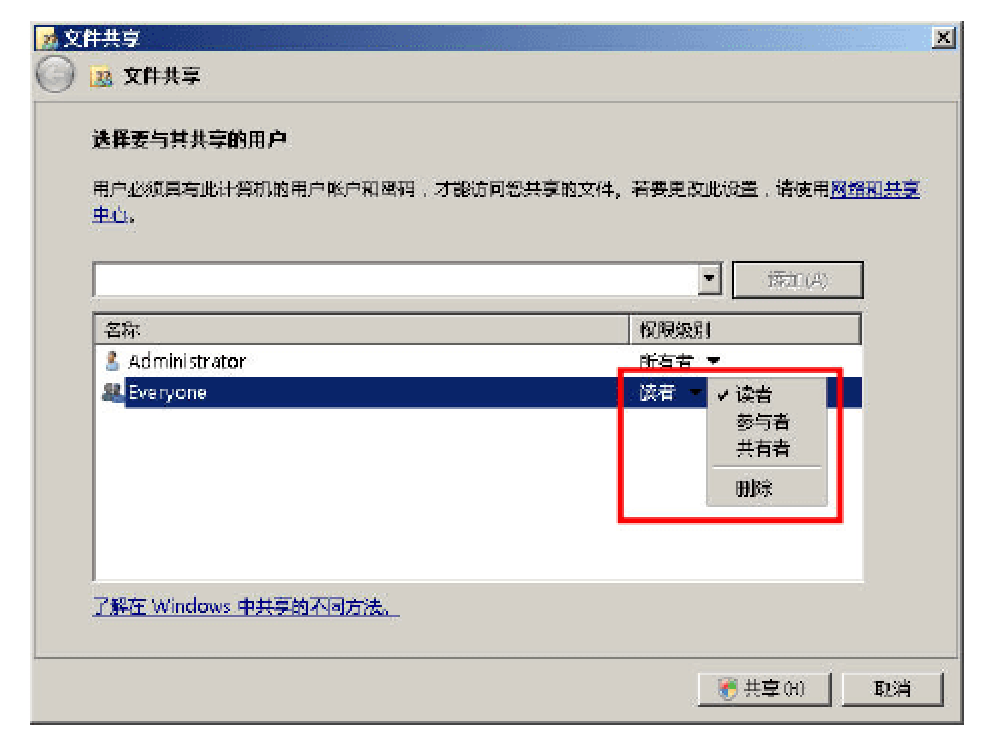


图 4-113　更改或添加权限

也可以单击“▼”下拉按钮，再次添加其他用户，然后在用户与权限列表中，修改或添加、删除权限。

05 在“您的文件夹已共享”对话框中，单击“完成”按钮，共享完成，如图 4-114 所示。图中同时显示了其他计算机访问该共享文件夹的路径，在本例中为\\WS08R2\software，其中 WS08R2 是服务器的计算机名称，software 是共享文件名称。在实际使用中，也可以用服务器的 IP 地址、DNS 名称，或者其他只要能解析到 WS08R2 的 IP 地址的名称都可以代替 WS08R2。

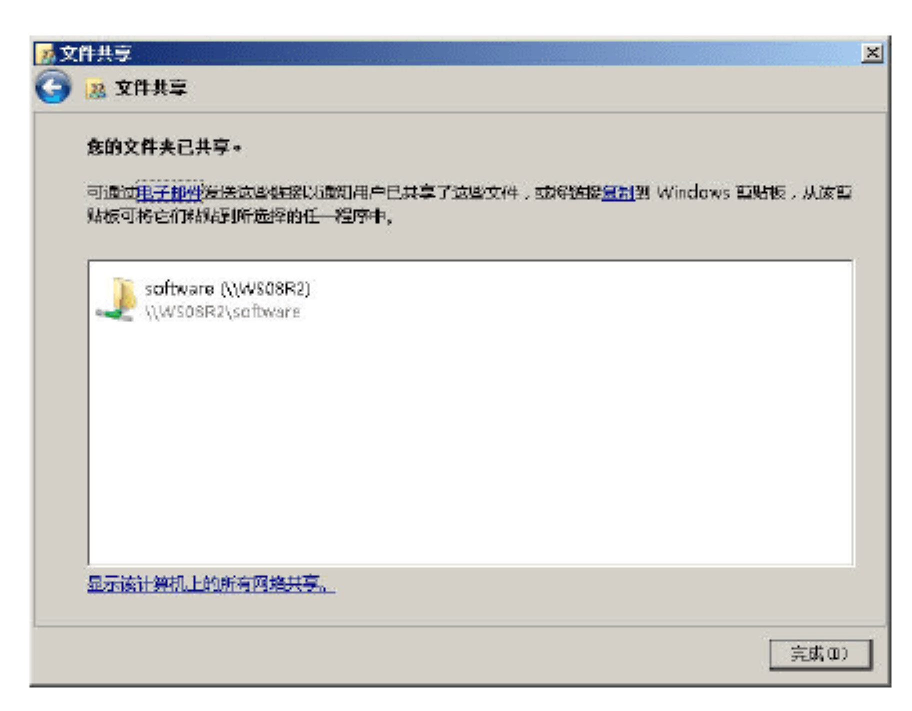


图 4-114 共享完成

4.9.3 创建隐含共享文件夹

如果要为一个文件夹创建多个共享名称，或者要创建“隐含”共享名称的共享文件夹，可以按照如下的步骤进行操作。

01 打开资源管理器，右击要创建共享的文件夹，在弹出的快捷菜单中选择“属性”命令，如图 4-115 所示。

02 在弹出的“software 属性”对话框中，在“共享”选项卡中，单击“高级共享”按钮，如图 4-116 所示。

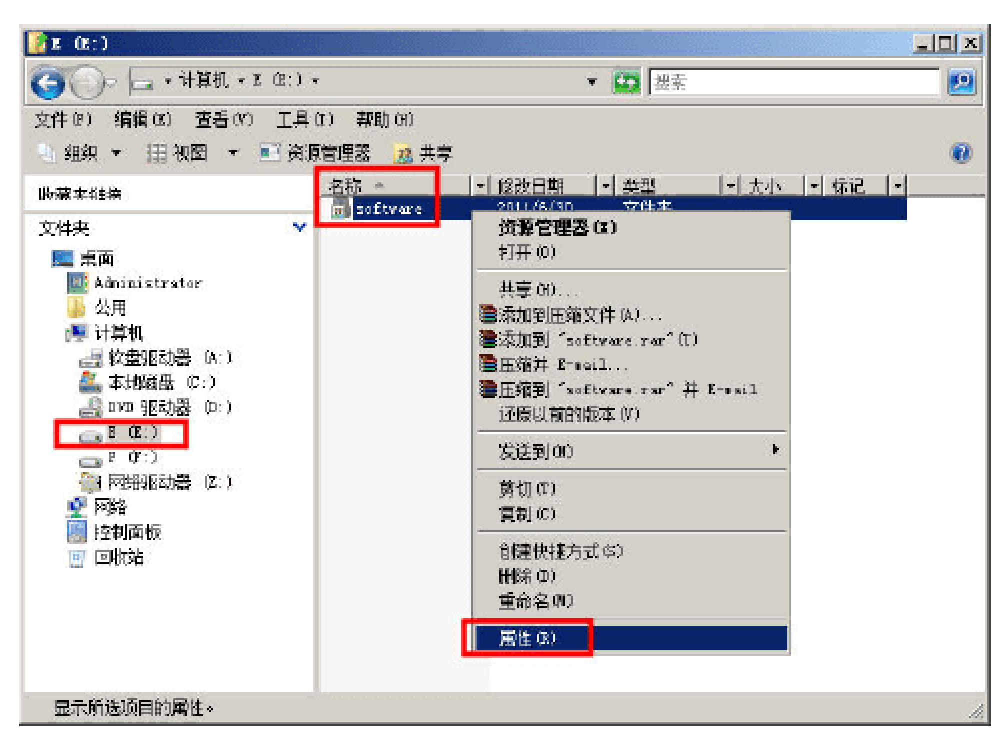


图 4-115 属性

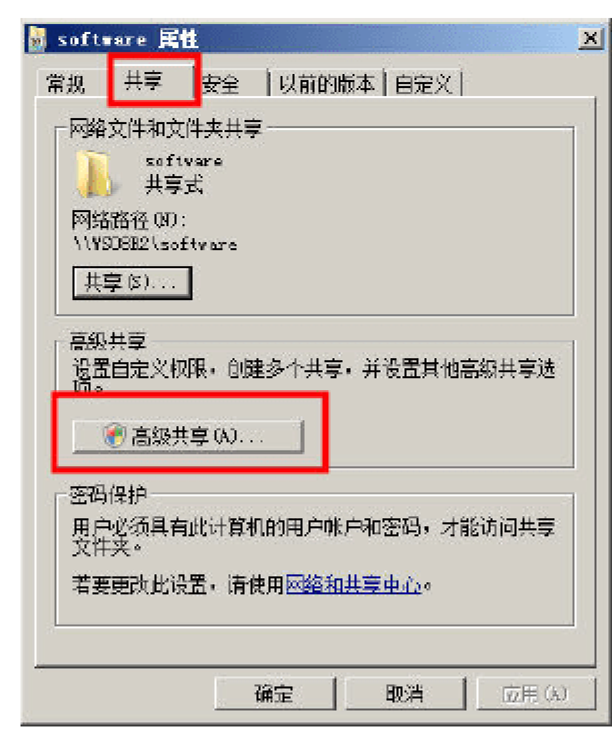


图 4-116 高级共享

03 在弹出的“高级共享”对话框中，单击“添加”按钮（如图 4-117 所示），在弹出的“新建共享”对话框中，在“共享名”文本框中，输入新的共享文件夹名称，如果要创建隐含共享，则在共享名后以$结尾，如图 4-118 所示。

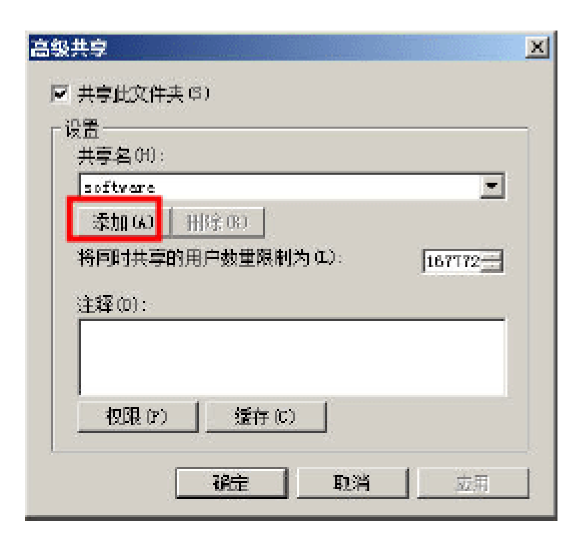


图 4-117 添加共享

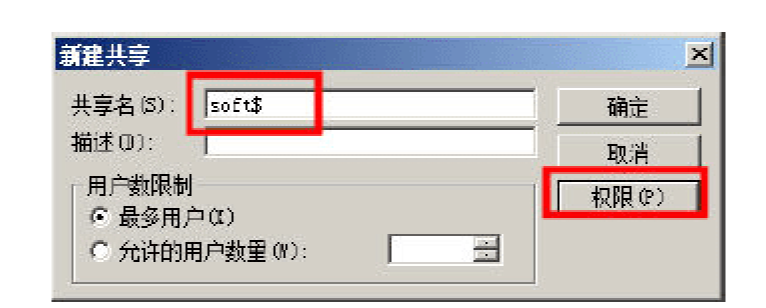


图 4-118 创建共享名

04 如果要修改共享权限，可以在图 4-118 中，单击“权限”按钮，将弹出“共享权限”对话框，在该对话框中，添加要共享的组名或用户，然后选中用户和组进行权限设置，如图 4-119 所示。

05 在设置完权限之后，三次单击“确定”按钮、然后单击“关闭”按钮，完成隐含共享文件夹的创建。

图 4-119　设置共享权限

4.9.4　测试共享文件夹

本小节测试前文创建的共享文件夹，主要步骤如下。

01 在网络中的其他计算机，或者在 Windows 2008 计算机中，打开“网络”（如果是 Windows XP、Windows Server 2003 则是“网上邻居”），浏览选择名为 WS08R2 的计算机，可以看到前文创建的名为 software 的共享，如图 4-120 所示。

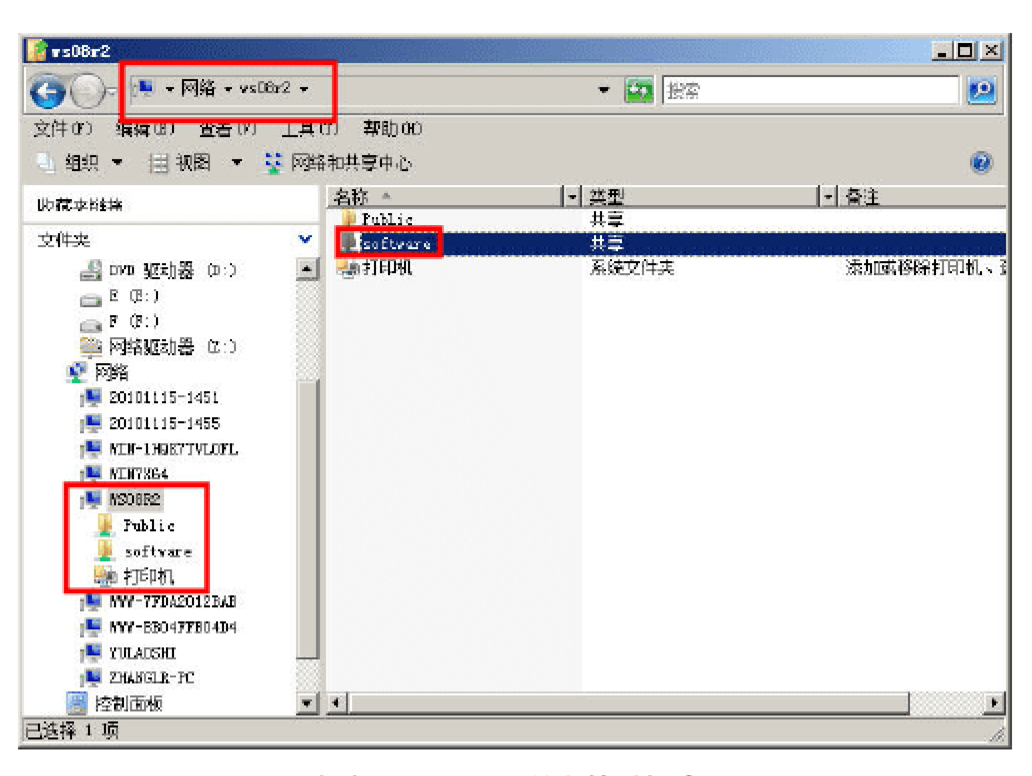
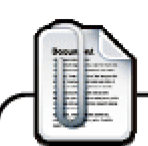


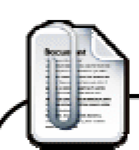
图 4-120　浏览共享



说 明

也可以打开资源管理器，通过输入“\\ws08r2”或“\\ws08r2”的 IP 地址（不包括双引号）然后按回车键的方式，直接“浏览”服务器的共享文件夹。

02 如果要使用“隐含”共享文件夹，只能通过直接输入共享服务器的名称（或 IP 地址、或 DNS 名称）再加入隐含共享文件夹名称的方式访问，例如，在本例中，可以通过在“地址栏”中输入\\ws08r2\soft$的方式，使用隐含共享文件夹，如图 4-121 所示。



说 明

在具有多个 VLAN 的网络中，如果客户端与服务器不在同一网段，在使用类似于 ws08r2 的 NetBIOS 名称时，需要在网络中配置 DNS 服务器或 WINS 服务器进行解析，否则会由于 VLAN 屏蔽广播的原因，导致不能以 NetBIOS 名称访问服务器。

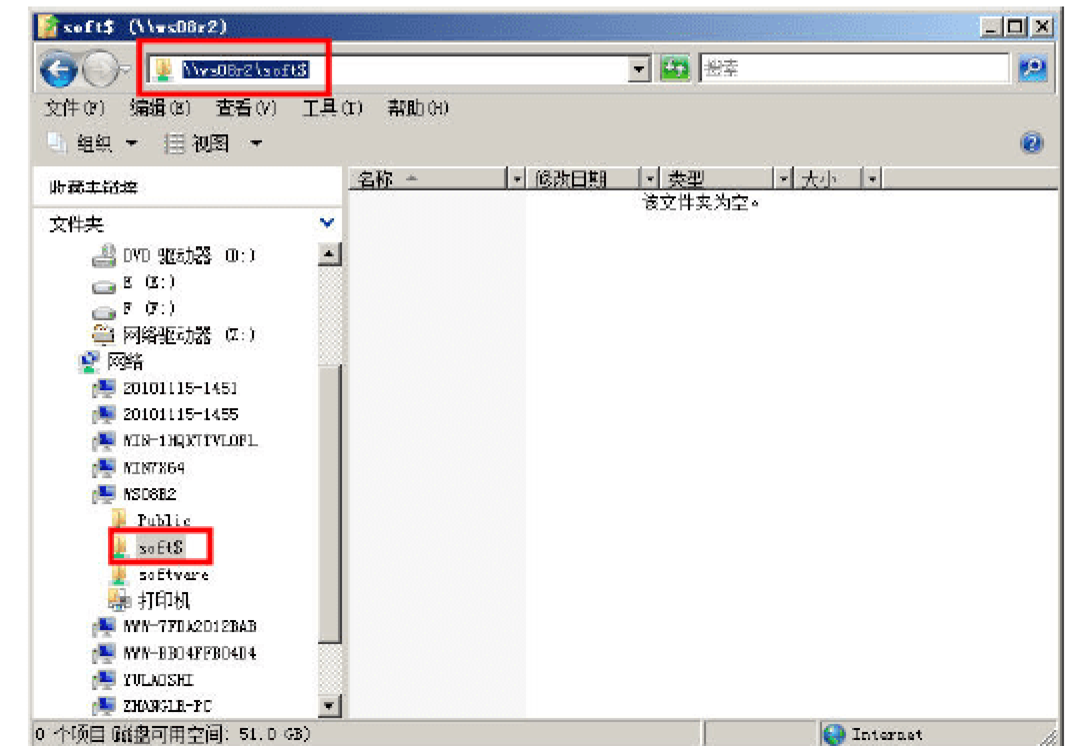


图 4-121　使用隐含共享文件夹

4.9.5　公用文件夹

在 Windows Vista、Windows 7、Windows Server 2008、Windows Server 2008 R2 中，还可以通过“公用文件夹”的方式，在多个用户之间共享数据。“公用文件夹”使用比较简单，如果能直接登录到服务器，可以直接打开“资源管理器”，然后定位到“桌面→公用”，将需要共享的数据复制到“公用文件夹”的不同目录之中即可，其他用户登录之后就可以访问或使用公用文件夹中的数据，如图 4-122 所示。

如果让用户通过网络访问服务器的“公用文件夹”，则可以将“公用文件夹”共享。共享公用文件夹的方式很简单，可以通过“4.9.2 创建共享文件夹”的方式，将“公用文件夹”共享，也可以打开“控制面板→网络和共享中心”，在“共享和发现”列表中，启用“公用文件夹共享”，如图 4-123 所示。

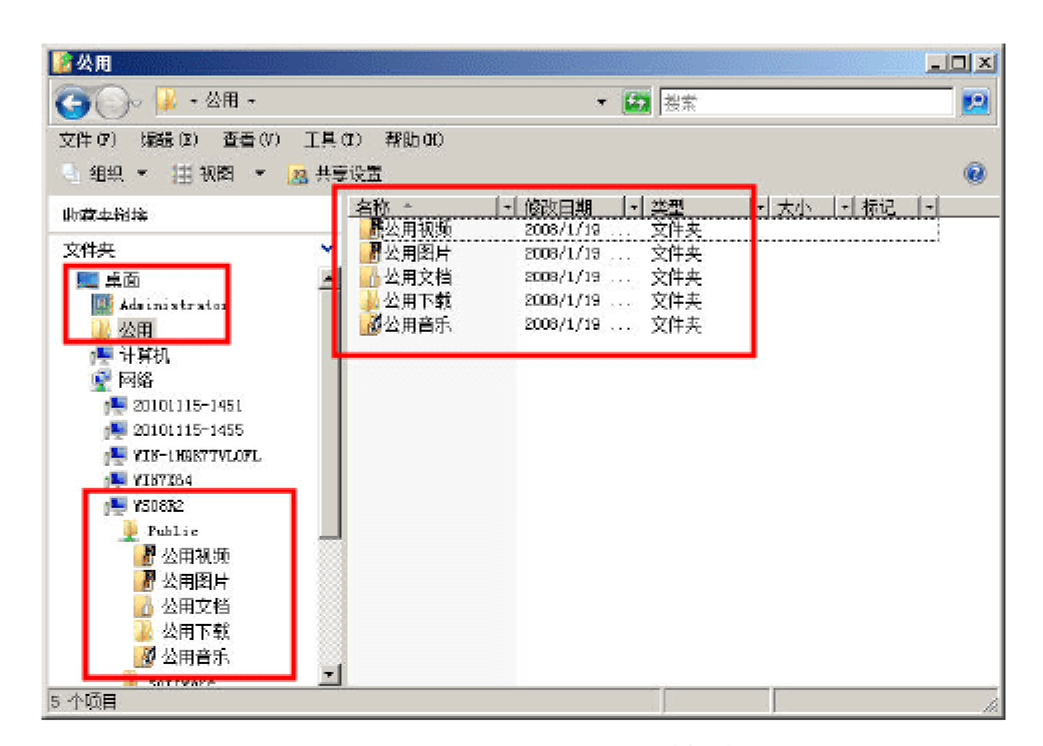


图 4-122　公用文件夹

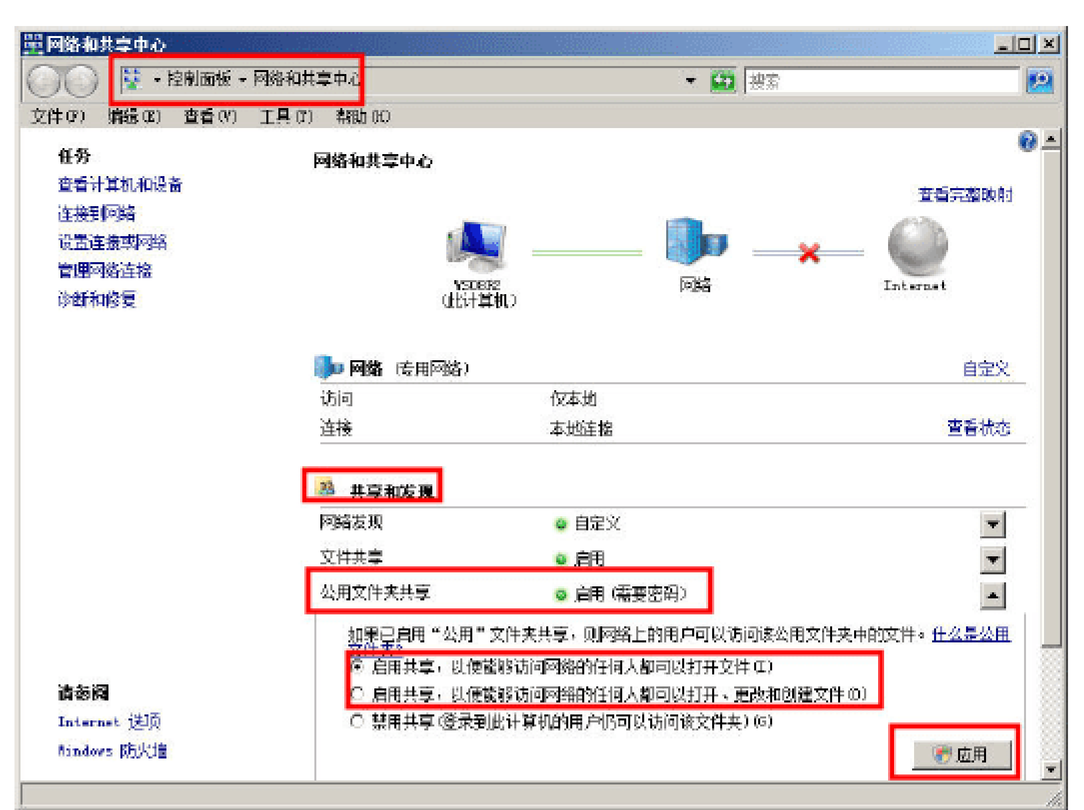


图 4-123　公用文件夹共享

4.10　卷影副本

“卷影副本”是在“共享文件夹”基础上的一种应用。共享文件夹的卷影副本提供位于共享资源（例如，文件服务器）上的实时文件副本。通过使用共享文件夹的卷影副本，用户可以查看在过去某个时刻存在的共享文件和文件夹。访问文件的以前版本或卷影副本非常有用，原因是用户可以实现下面的操作。

- 恢复被意外删除的文件。如果用户意外删除了某个文件，则可以打开以前的版本，然后将其复制到安全的位置。
- 恢复意外覆盖的文件。如果用户意外覆盖了某个文件，则可以恢复该文件的前一版本。
- 在处理文件的同时对文件版本进行比较。当用户希望检查一个文件的两个版本之间发生的更改时，可以使用以前的版本。

4.10.1　使用卷影副本的注意事项

使用卷影副本的注意事项如下：

（1）当用户恢复文件时，文件权限不会更改，权限在恢复前后没有变化。当用户恢复一个意外删除的文件时，文件权限将被设为该目录的默认权限。

（2）创建卷影副本不能替代创建常规备份。

（3）当存储区域达到限制值之后，将删除最旧的卷影副本，从而留出空间以便创建更多卷影副本。删除卷影副本之后，将无法检索该副本。

（4）可以调整存储位置、空间分配和计划以满足需要。在“本地磁盘属性”对话框的“卷影副本”选项卡上，单击“设置”按钮。

（5）每个卷上最多可以存储 64 个卷影副本。达到该限制值之后，将删除最旧的卷影副本，且无法检索该副本。

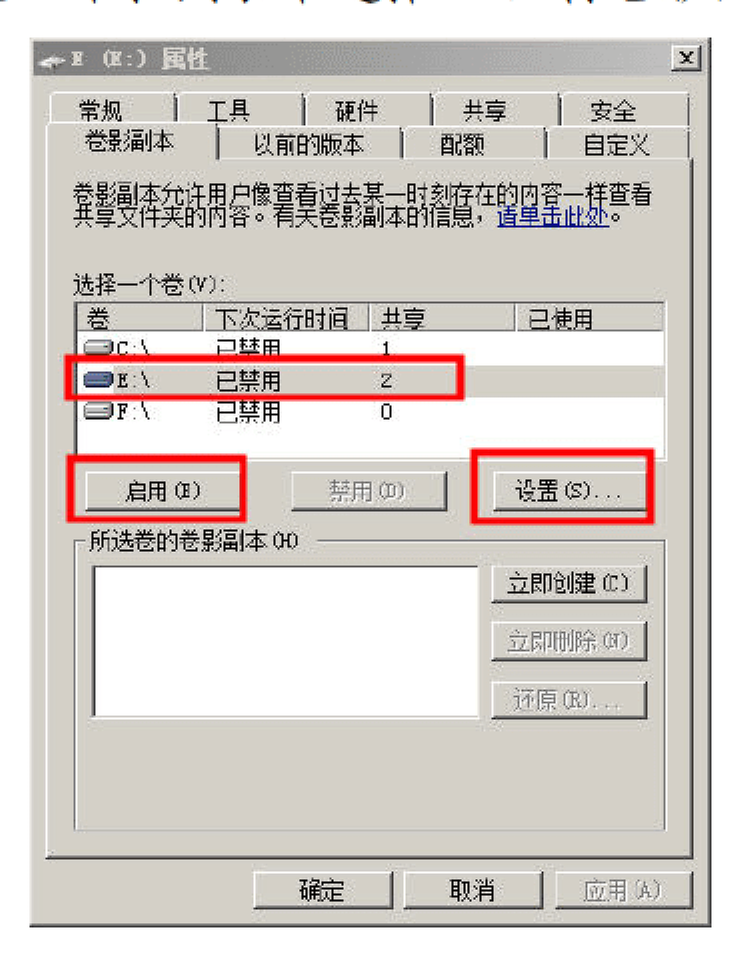
（6）卷影副本是只读的。不能编辑卷影副本的内容。

（7）只能针对每个卷启用共享文件夹的卷影副本，也就是说，不能在卷上选择要进行复制或不进行复制的特定共享文件夹和文件。

4.10.2 启用卷影副本功能

本小节以在 E 盘的 software 共享文件夹、在 F 盘启用卷影副本为例，介绍启用卷影副本的方法，步骤如下。

01 打开“资源管理器”，右击 E 盘，在弹出的快捷菜单中选择“属性”，打开 E 盘属性对话框，单击“卷影副本”选项卡，选中 E 盘，单击“设置”按钮，在弹出的“设置”对话框中，在“位于此卷”下拉列表中选择 F:\，将卷影副本保存于 F 盘，如图 4-124 所示。



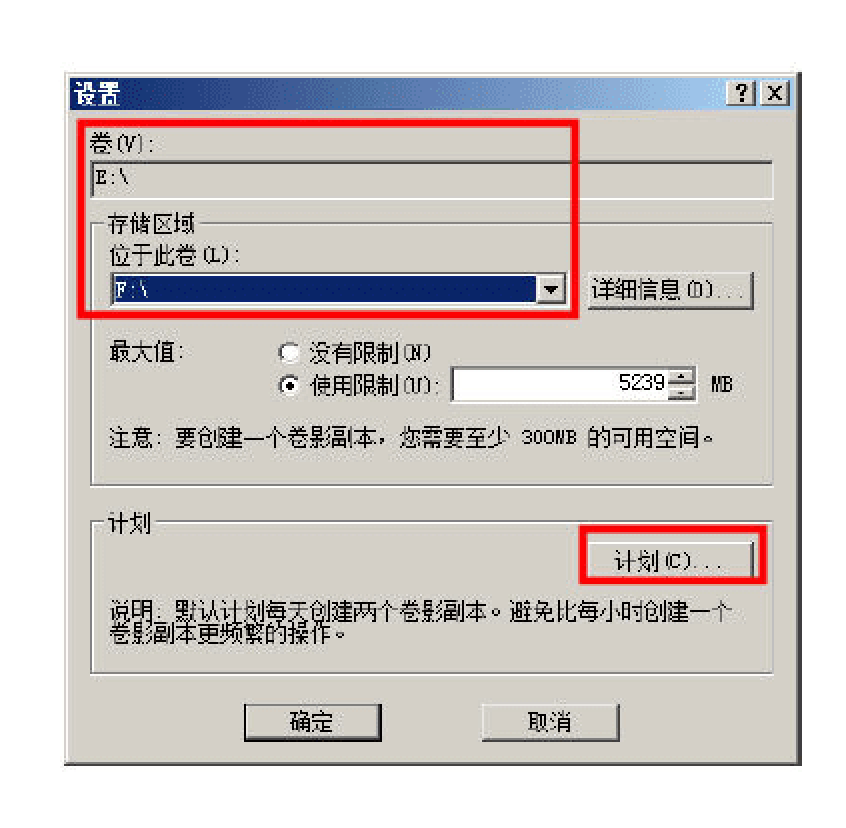


图 4-124 设置卷影副本

02 如果要修改创建卷影副本的安排，则单击“计划”按钮，在弹出的对话框中，可以根据管理员的需要，设置创建卷影副本的间隔时间，如图 4-125 所示。可以删除系统默认的时段，然后单击“新建”按钮，创建新的计划。

如果使用默认值启用卷上的共享文件夹的卷影副本，系统会计划任务，在上午 7:00 和中午 12:00 时创建卷影副本。默认存储区域将位于同样的卷上，而且其大小将是可用空间的 10%。

设置好计划之后，单击“确定”按钮，再次单击“确定”按钮，返回到 E 盘属性对话框。

03 在启用卷影副本之后，系统将会在图 4-125 中指定的时刻，自动创建卷影副本。在启用卷影副本时，只能针对每个卷启用共享文件夹的卷影副本，也就是说，不能在卷上选择要进行复制或不进行复制的特定共享文件夹和文件。

04 如果要立刻创建卷影副本，可以单击“立既创建”按钮，随时创建共享文件夹的即时快照。也可以选中不需要的卷影副本，单击“立既删除”按钮，删除不需要的卷影副本。也可以选中一个副本，单击“还原”按钮，将共享文件夹中的数据恢复到快照时间点，如图 4-126 所示。

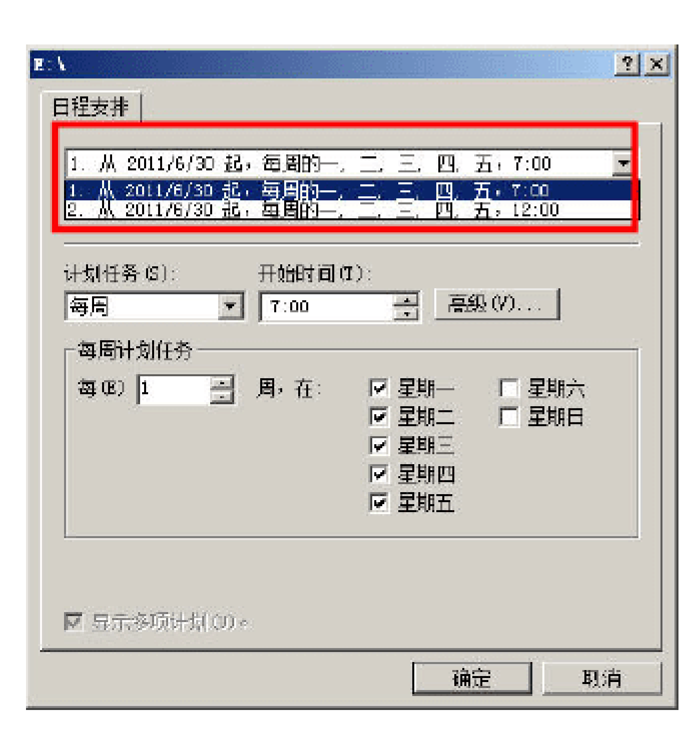


图 4-125　创建计划

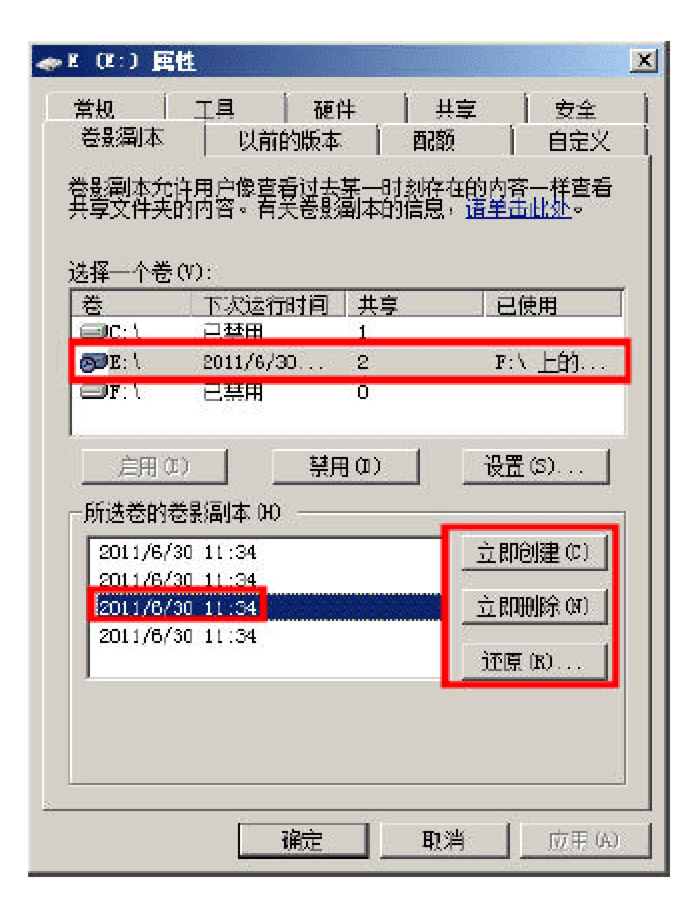


图 4-126　管理卷影副本



说 明

如果在图 4-126 中，对卷影副本进行了还原，则 E 盘共享文件夹中的数据会恢复到还原时的状态，以后时刻的卷影副本将会被删除，并且不能再被恢复。

05 对于普通用户来说，当通过网络使用共享文件夹，访问具有卷影副本功能的共享文件夹时，可以在共享文件夹的“属性”（如图 4-127 所示）对话框中，在“以前的版本”选项卡中，查看创建的多个卷影副本，如图 4-128 所示。

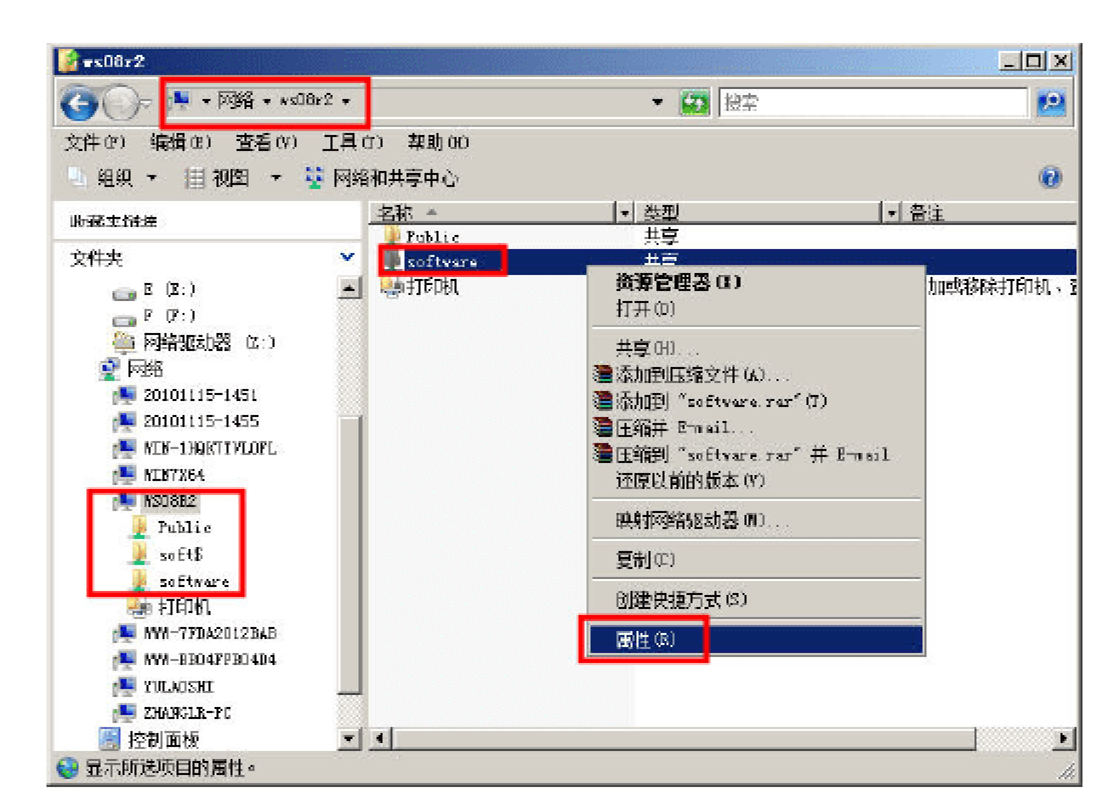


图 4-127　共享文件夹属性

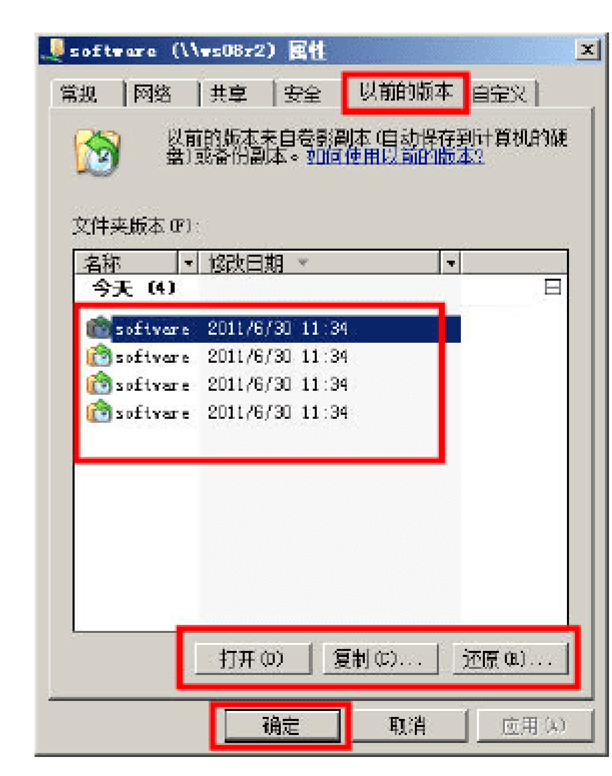


图 4-128　以前的版本

06 用户可以在图 4-128 中，选中一个卷影副本时间点，然后单击“打开”按钮，查看“快

照”时的共享文件夹中的内容，如图 4-129 所示。此时，可以在打开的卷影副本处，复制、查看当时的状态。

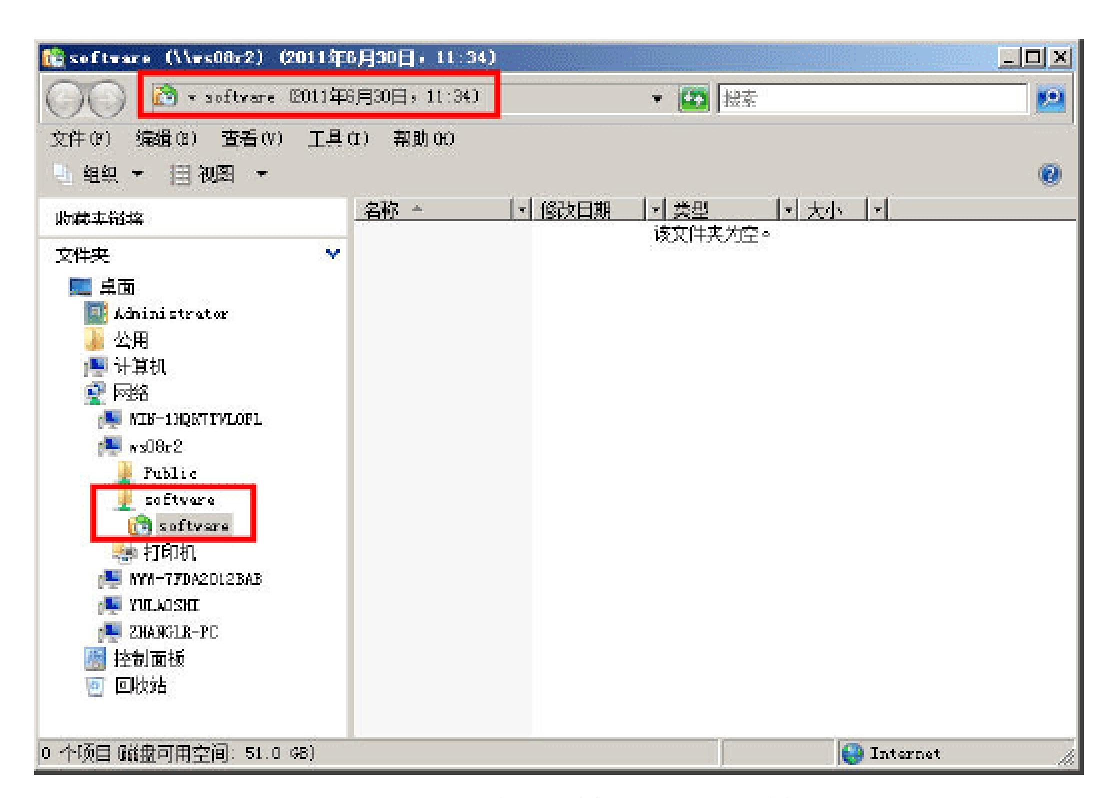


图 4-129　查看快照时的数据

4.10.3　卷影副本的最佳操作

为了充分发挥卷影副本的功能与效果，推荐采用如下操作方式。

（1）最好不要在同一个磁盘上启用卷影副本，推荐在另一个磁盘上选择一个单独的卷作为卷影副本的存储区域。

在未进行卷影复制的磁盘上选择一个存储区域。如果使用另一个磁盘上单独的卷，将不会发生高 I/O 负载导致卷影副本被删除的情况，而且会大大提高性能。对于使用率高的服务器，这是推荐的配置。

（2）启用共享文件夹的卷影副本并设置计划选项之前，确定客户端使用共享资源的方式。调整卷影副本计划以适合客户端的工作模式。

（3）不要在使用装入点的卷上启用卷影副本。

当获取卷影副本时，安装的驱动器将不包括在内。仅在没有装入点的卷上启用卷影副本，或者在不希望对安装卷上的共享资源进行卷影复制时启用卷影副本。

（4）对文件服务器执行常规备份。

共享文件夹的卷影副本不能替代执行常规备份。将备份实用程序和共享文件夹的卷影副本结合使用，作为最佳恢复准备。

（5）不要将副本计划为每小时发生多次。

创建卷影副本的默认计划是周一到周五的早上 7:00 和中午。如果决定要更频繁地获取副本，须确认已分配了足够的存储空间，以及你的复制频率不会导致服务器性能降低。另外，副本计划还有一个上限，即每个卷最多可以存储 64 个副本，达到这个限制之后将删除最旧的副本。如果获取卷影副本太过频繁，可能会很快达到该限制值，时间较早的副本也会很快丢失。

（6）在删除进行卷影复制的卷之前，要先删除用于创建卷影副本的计划任务。

如果在没有删除卷影副本任务的情况下删除卷，计划任务就会失败，事件日志中就会写入一个事件 ID 为 7001 的错误。在删除卷之前先删除任务，可避免事件日志中写入这种错误。

（7）在格式化将要启用共享文件夹的卷影副本的源卷时，使用 16KB 或更大的分配单元。

如果计划对启用共享文件夹的卷影副本的源卷进行磁盘碎片整理，建议在初次对源卷进行格式化时，将群集分配单元的大小设为 16 KB 或更大。如果不这样做，由磁盘碎片整理引起的数量更改可能会导致以前版本的文件被删除。

如果需要在源卷上压缩 NTFS 文件，则不能使用大于 4 KB 的分配单元。因为在这种情况下，当对非常零碎的卷进行磁盘碎片整理时，可能会更快丢失较旧的卷影副本。

第 5 章　Internet 信息服务器管理与应用

Internet 信息服务器（Internet Information Server，简称 IIS）是 Windows Server 中的“Web 服务器”，它包括了 Web（网站）服务器与 FTP（文件传送）服务器两部分的功能。本节介绍如何使用 IIS 创建、配置 Web 与 FTP 服务器。

5.1　Web 服务器概述

通过 Windows Server 2008 R2 中的 Web 服务器角色，用户可以与 Internet、Intranet 或 Extranet 上的其他用户共享信息。Windows Server 2008 提供了 IIS 7.0，Windows Server 2008 R2 集成了 IIS 7.5。IIS 是一个集成了 IIS、ASP.NET、Windows Communication Foundation 的统一 Web 平台。

Web 服务器是指具有允许它们接受和响应来自客户端计算机的请求的特定软件的计算机。Web 服务器允许用户通过 Internet 或 Intranet 和 Extranet 共享信息。

通过 Web 服务器，可以实现下面操作：

- 向 Internet 上的用户提供信息。
- 允许用户利用 FTP 或万维网分布式创作和版本控制（WebDAV）下载和上载内容。
- 承载包含三层应用程序的业务逻辑的 Web 服务。
- 通过 Internet 而不是软盘或 CD 等物理介质向用户分发应用程序。

Web 服务器可供不同的用户使用，并能满足不同的需要。例如：

- 小型企业可能会使用简单的网站来提供有关其服务的信息。
- 中型企业可能会通过站点内的各种应用程序编译的在线订购系统来提供产品和服务。
- 大型企业可能会通过企业 Intranet 为员工开发和提供业务应用程序。
- 托管公司可能会为各个客户提供服务器空间和服务以承载不同的联机内容和应用程序。
- 合资企业可能会通过 Extranet 为业务合作伙伴提供相关信息和应用程序。

Web 与 FTP 服务器，也是典型的“客户/服务器”系统结构，通常情况下，根据用户的需求不同，Web 服务器可能有以下三种应用，下面分别介绍。

第一种，Web 服务器用于企业内部局域网。在企业内部的服务器中，安装配置 Web 与/或 FTP 服务器，企业内部的用户通过 IP 地址或者内部的域名访问 Web 服务器，网络拓扑如图 5-1 所示。

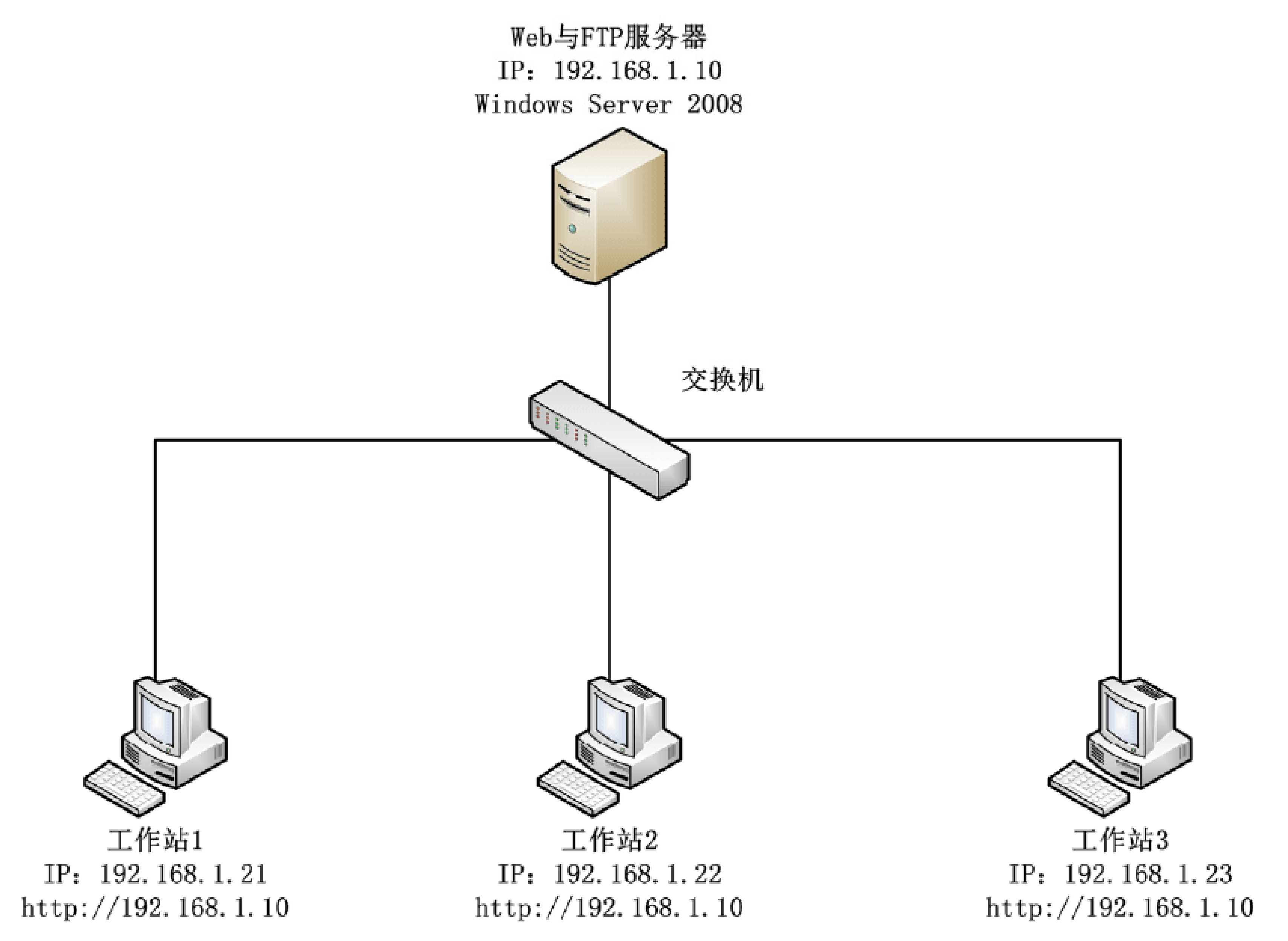


图 5-1　在企业内部中的 Web 服务器

在图 5-1 中，Web 服务器的 IP 地址是 192.168.1.10，企业内部的其他计算机可以直接使用 http://192.168.1.10 的方式，访问企业内部的 Web 服务器。

第二种，Web 服务器托管或放置在具有公网 IP 地址的机房中，Internet 的用户通过域名或 IP 地址，访问该 Web 服务器提供的网站，网络拓扑如图 5-2 所示。

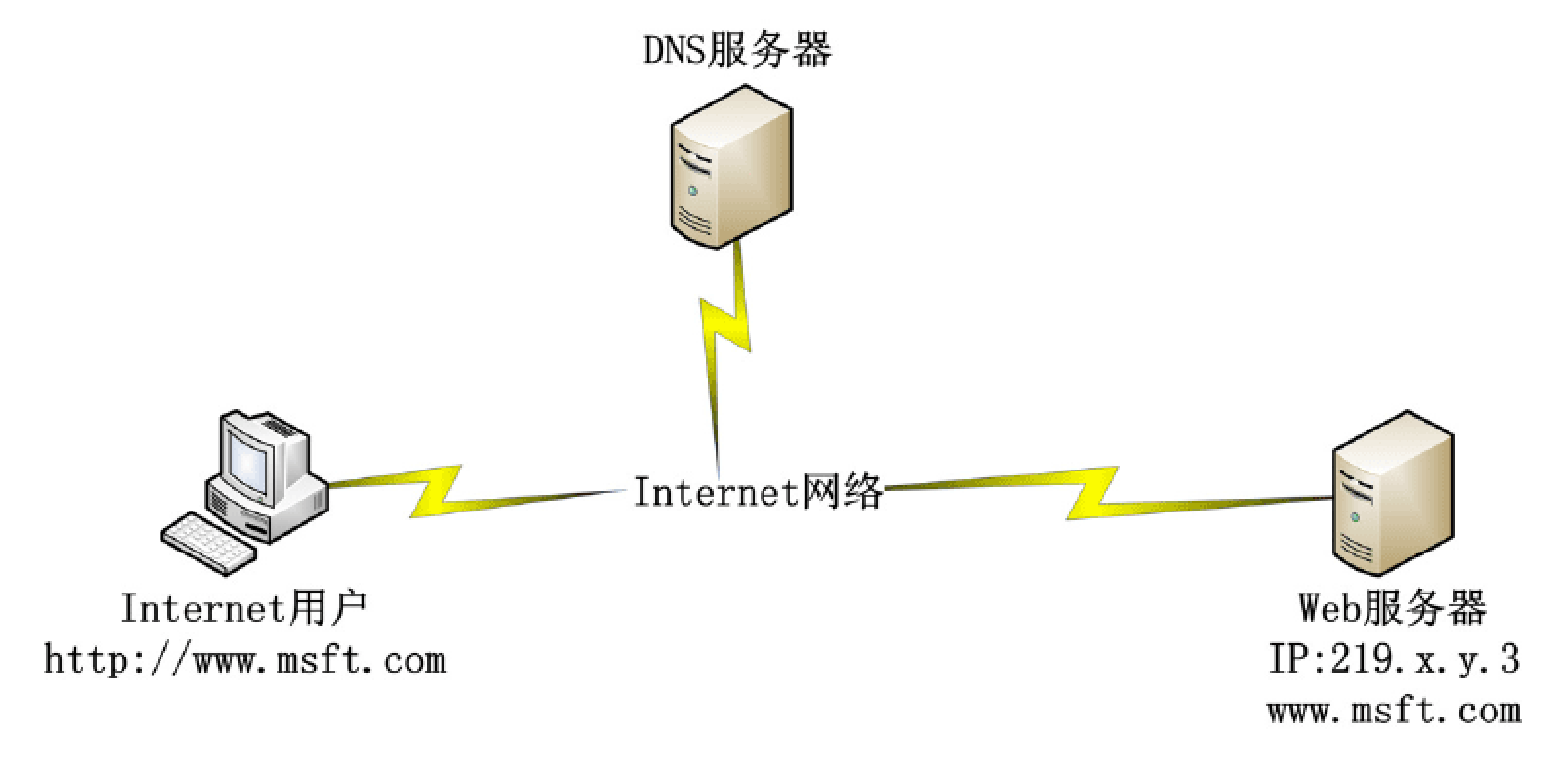


图 5-2　放置在公网上的 Web 服务器

在图 5-2 中，IP 地址为 219.x.y.3 的服务器上，放置了域名为 www.msft.com 的网站。当 Internet 上的用户试图通过 www.msft.com 访问该网站时，首先要从 DNS 服务器解析到 219.x.y.3 的 IP 地址，才能访问该网站。

第三种则是前两种的组合应用。企业的 Web 服务器，放置在自己的机房中，除了让企业内部的用户访问外，还通过防火墙发布到 Internet，供 Internet 的用户访问，网络拓扑如图 5-3 所示。

在图 5-3 中，Web 服务器在企业网络中的 IP 地址是 192.168.1.10，防火墙对外地址是 219.x.y.3。该 Web 服务器通过防火墙发布到 Internet 中。当企业内部用户访问时，可以通过内部的 IP 地址

http://192.168.1.10 或通过内部的域名 http://www.msft.com 访问。在企业内部，DNS 被设置为 192.168.1.9，该 DNS 服务器将 www.msft.com 解析为 192.168.1.10。在 Internet 网络中，Internet 用户使用域名 http://www.msft.com 访问到 219.x.y.3 的防火墙，该防火墙将 Internet 用户的访问转发到 192.168.1.10 的 Web 服务器，完成对用户的服务。

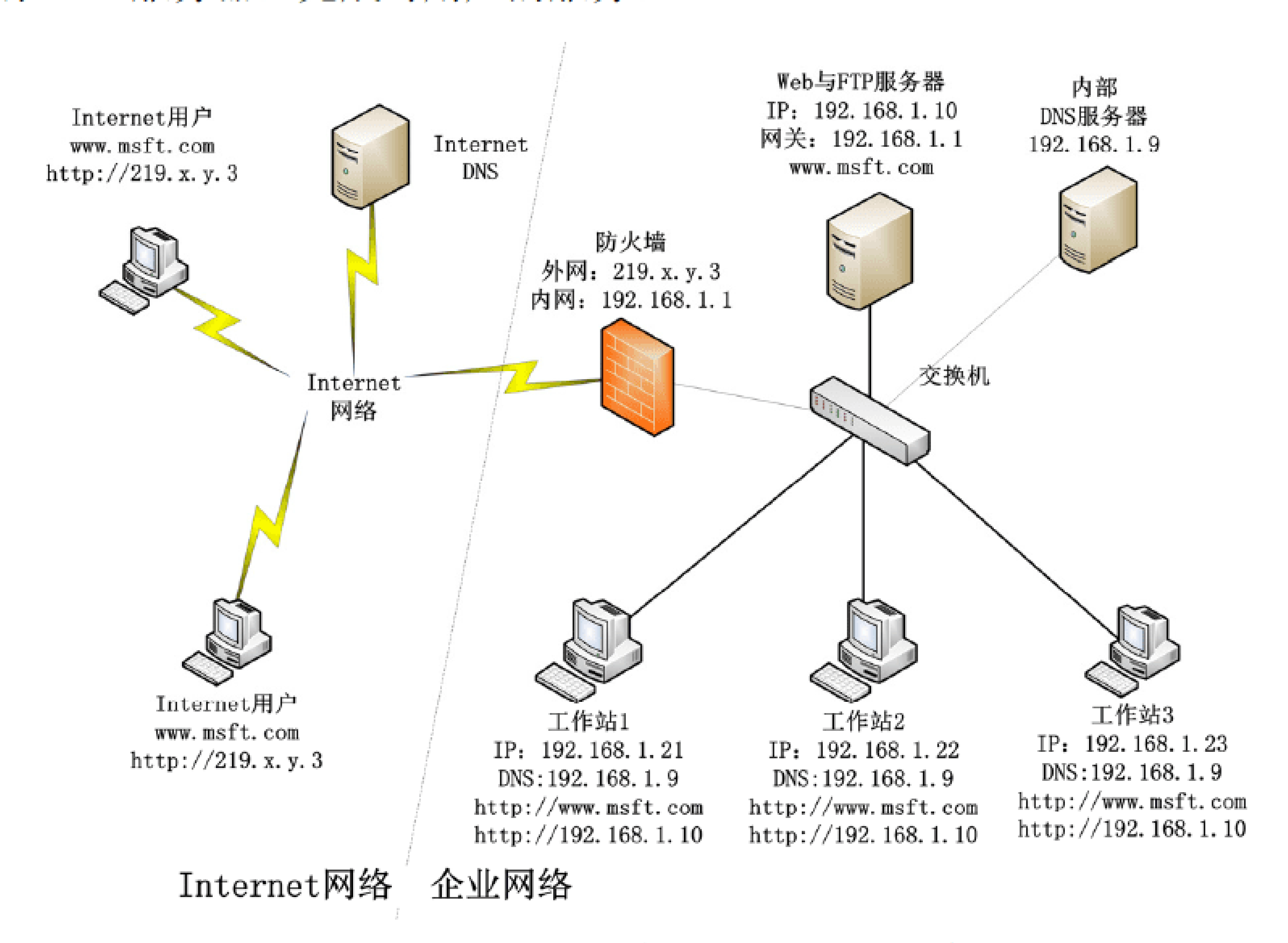


图 5-3　供 Internet 与企业访问的 Web 服务器

通过这三种方式可以看到，无论是哪种方式，对于 Web 服务器来说，只要配置好网站（Web 与/或 FTP），其他问题则是防火墙或 DNS 解析的问题。所以，本章接下来将介绍 Web 与 FTP 服务器的安装、配置。

5.2　安装 Web 服务器

在 Windows Server（包括以前的 Windows 2000 Server、Windows 2003 Server、现在的 Windows Server 2008、Windows Server 2008 R2）中，大多数的服务是基于“组件”（Windows Server 2003 及其以前的叫法）或“角色”（Windows Server 2008 及其以后）的方式组成，并且在需要的时候添加，不需要的时候卸载。在 Windows Server 2008 及 Windows Server 2008 R2 中，大多数的服务器都是通过添加角色的方式来添加的。

在 Windows Server 2008 R2 中，Web 服务器是一个集成了许多功能的服务器，可以在添加 Web 服务器的时候，根据用户的需求，选择某个或某些功能。下面介绍添加 Web 服务器的方法与步骤。

01 以管理员的身份登录到 Windows Server 2008 R2，打开“服务器管理器”窗口，右击“角色”，在弹出的快捷菜单中选择“添加角色”选项（如图 5-4 所示），或者在右侧的角色列表中单击“添加角色”链接，都可以进入添加角色向导。

02 在“选择服务器角色”对话框中，选中“Web 服务器”复选框，此时将会弹出“添加角

色向导→是否添加 Web 服务器（IIS）所需的功能”对话框，单击“添加必需的功能”按钮，如图 5-5 所示。



图 5-4　添加角色

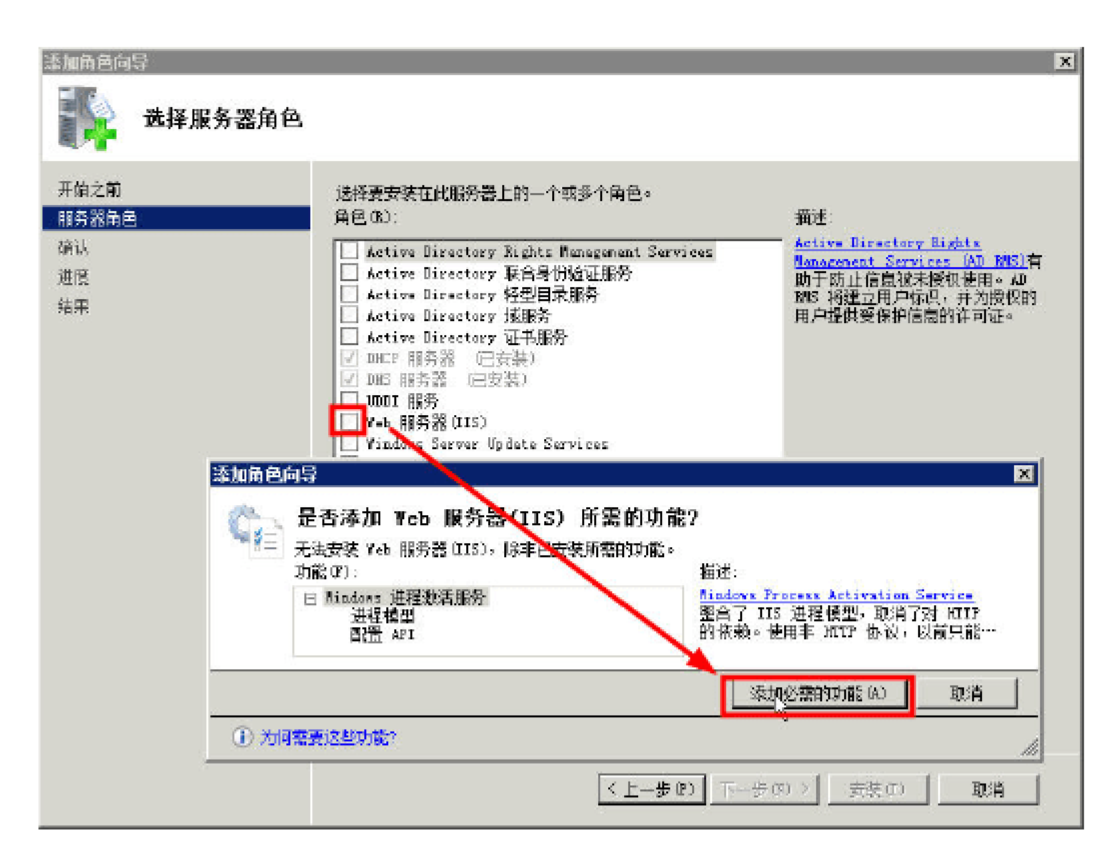


图 5-5　添加必需的功能

说 明

“添加必需的功能”是 Windows Server 2008 及 Windows Server 2008 R2 的一项新改进。当用户在安装一个产品或一个软件、或一个功能的时候，如果 Windows 检测到系统缺少必要的支持软件，则会弹出该对话框，提示并可以自动安装所需要的软件。以后，如果在安装软件的过程中，出现该类似提示，应单击“添加必需的功能”按钮，这样可以避免安装的软件出现问题。

这个功能应该是借鉴了 Linux 的 Yum 软件包管理的功能（Yum，全称为 Yellow dog Updater Modified，是一个在 Fedora 和 RedHat 以及 SUSE、CentOS 中的 Shell 前端软件包管理器。它基于 RPM 包管理，能够从指定的服务器自动下载 RPM 包并且安装，可以自动处理依赖性关系，并且一次安装所有依赖的软体包，无须繁琐地多次下载、安装）。

03 在“Web 服务器（IIS）”简介中，显示了 Web 服务器的简介及注意事项，阅读之后，单击“下一步”按钮，如图 5-6 所示。



图 5-6　Web 服务器简介

04 在“选择角色服务”对话框，在“角色服务”列表，选择要安装的 Web 服务器的对应功能。在此，选择每一个服务及功能，如图 5-7、图 5-8 所示。在实际的应用中，可根据需要选择。

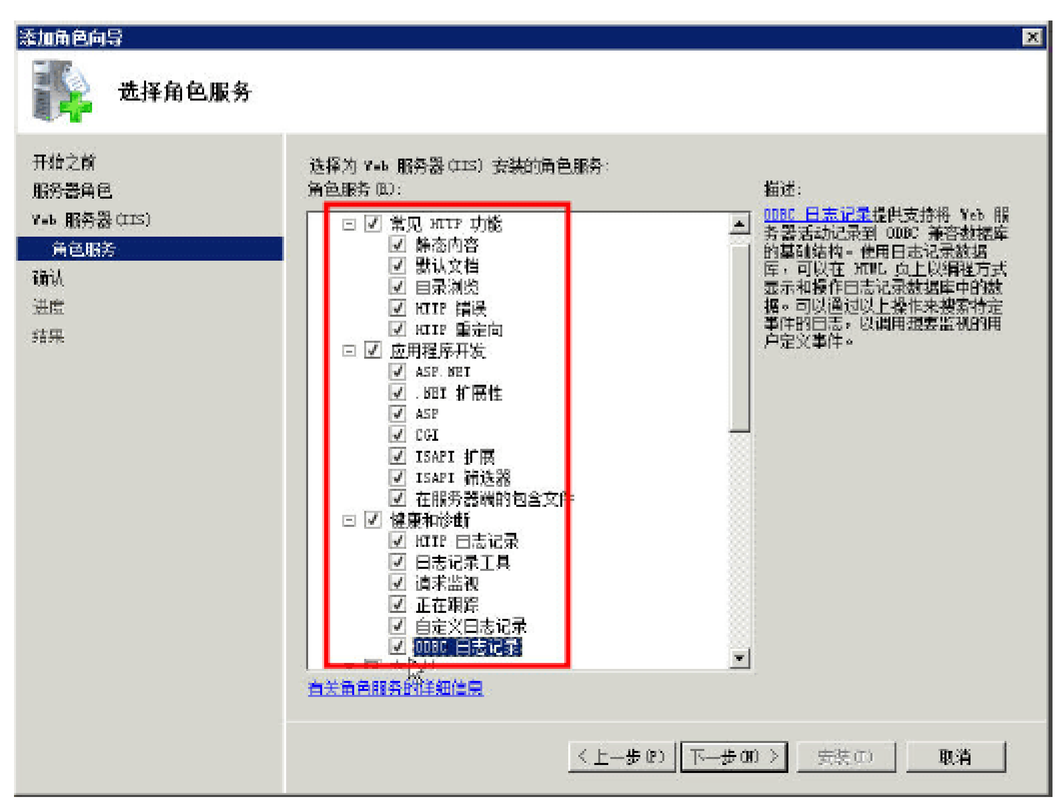


图 5-7　选择 Web 角色 1

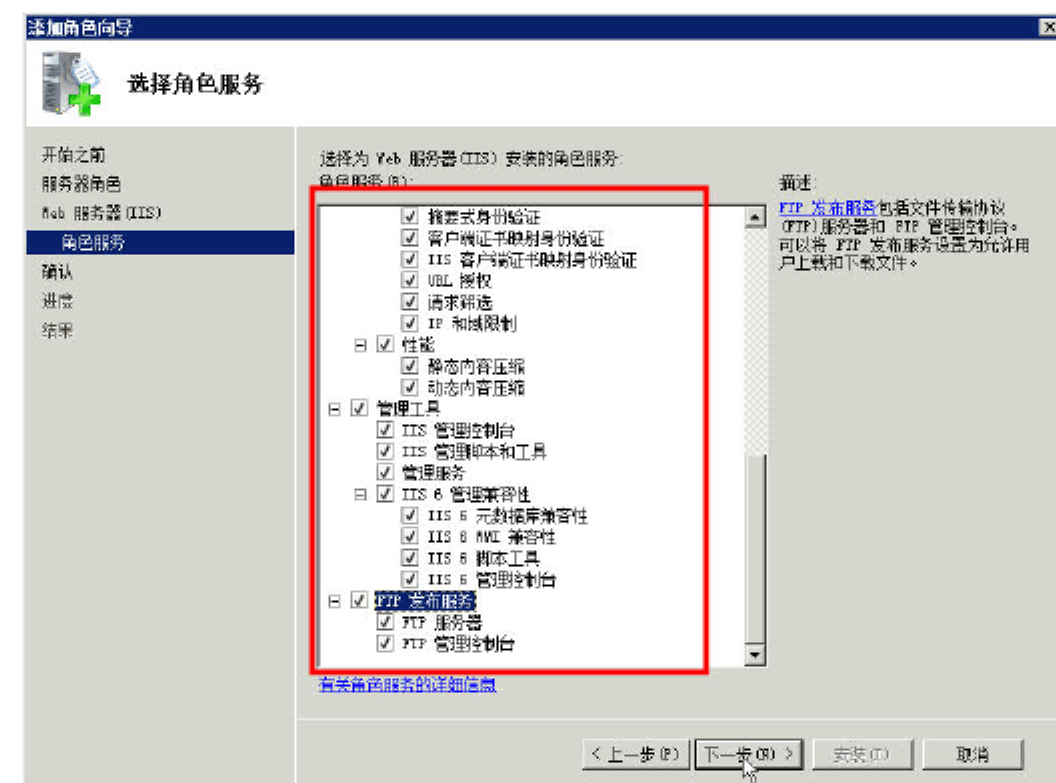


图 5-8　选择 Web 角色 2

05 在“确认安装选择”对话框，显示了当前要安装的 Web 服务器及功能，检查无误之后，单击“安装”按钮，开始安装，如图 5-9 所示。

06 安装完成之后，在“安装结果”对话框，显示安装的 Web 服务及功能，如图 5-10 所示。单击“关闭”按钮，完成安装。



图 5-9　确认安装选择



图 5-10　安装完成

在安装完 Web 服务器之后，新安装的 Web 服务器出现在“服务器管理器→角色→Web 服务器（IIS）”中，用户可以在此管理并配置 Web 服务器。安装 Web 不需要重新启动，可以立即使用。

如果以后想对 Web 服务器的角色进行删除或添加，可以定位到“服务器管理器→角色→Web 服务器（IIS）”，在右侧的“角色服务”列表中，单击“删除角色服务”或“添加角色服务”链接（如图 5-11 所示），会进入“选择角色服务”对话框，可以对 Web 服务器的功能进行删除或添加，如图 5-12 所示。

除了可以添加或删除角色服务外，在“服务器管理器→角色→Web 服务器（IIS）”右侧的“摘要”列表中，还可以查看 Web 服务器的事件、管理 Web 服务器相关的服务等，如图 5-13 所示。

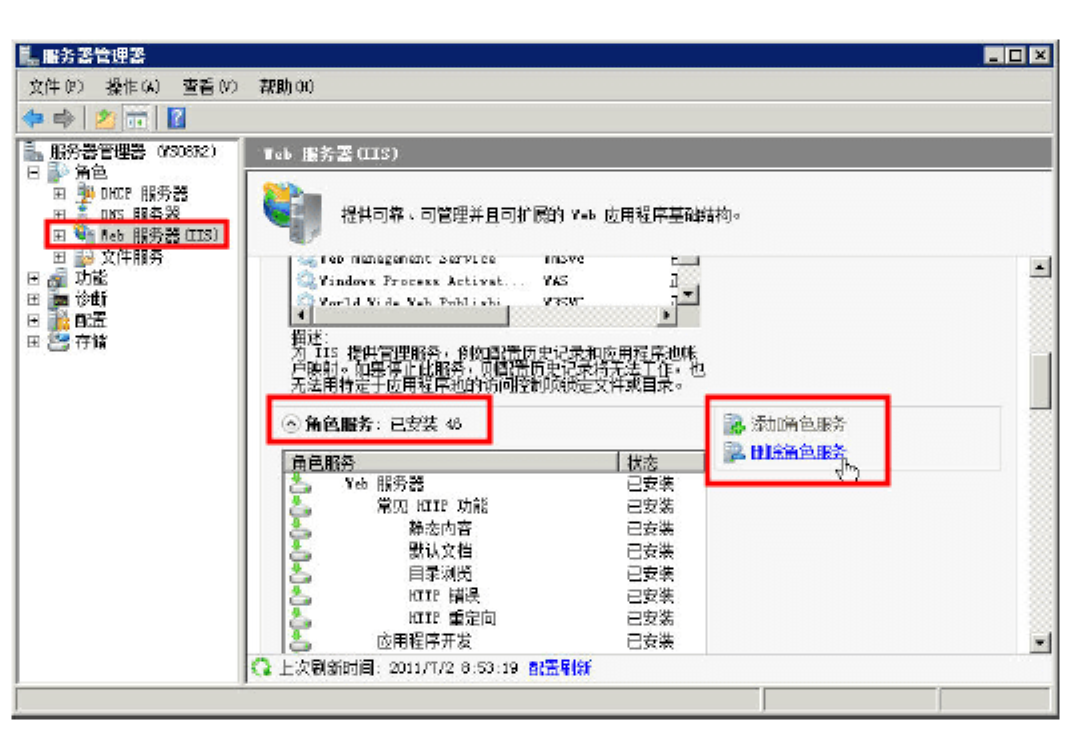
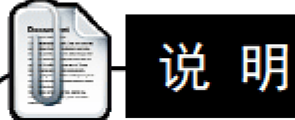




图 5-11　添加或删除角色服务



图 5-12　选择角色服务



说 明

从 Windows Server 2008 开始，大多数的服务器（如 DHCP、DNS、Web 服务器、文件服务器等），已经集成在“服务器管理器”中，并且每项服务都集成了“事件查看器”、“系统服务”、添加或删除角色、“资源和服务”等功能，以方便用户管理、使用对应的服务。

在安装好 Web 服务器之后，打开 IE 浏览器，输入 localhost，按回车键，出现如图 5-14 所示的信息，表示 Web 服务器安装正确。

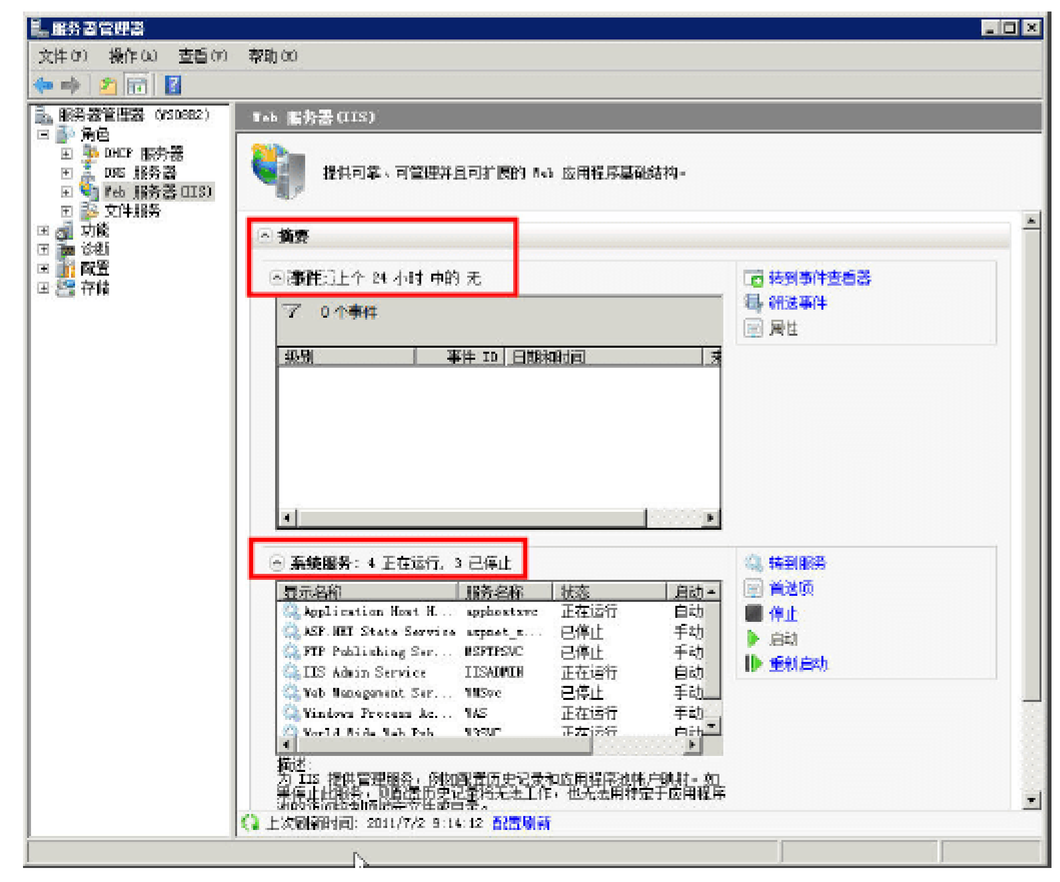


图 5-13　Web 服务器摘要

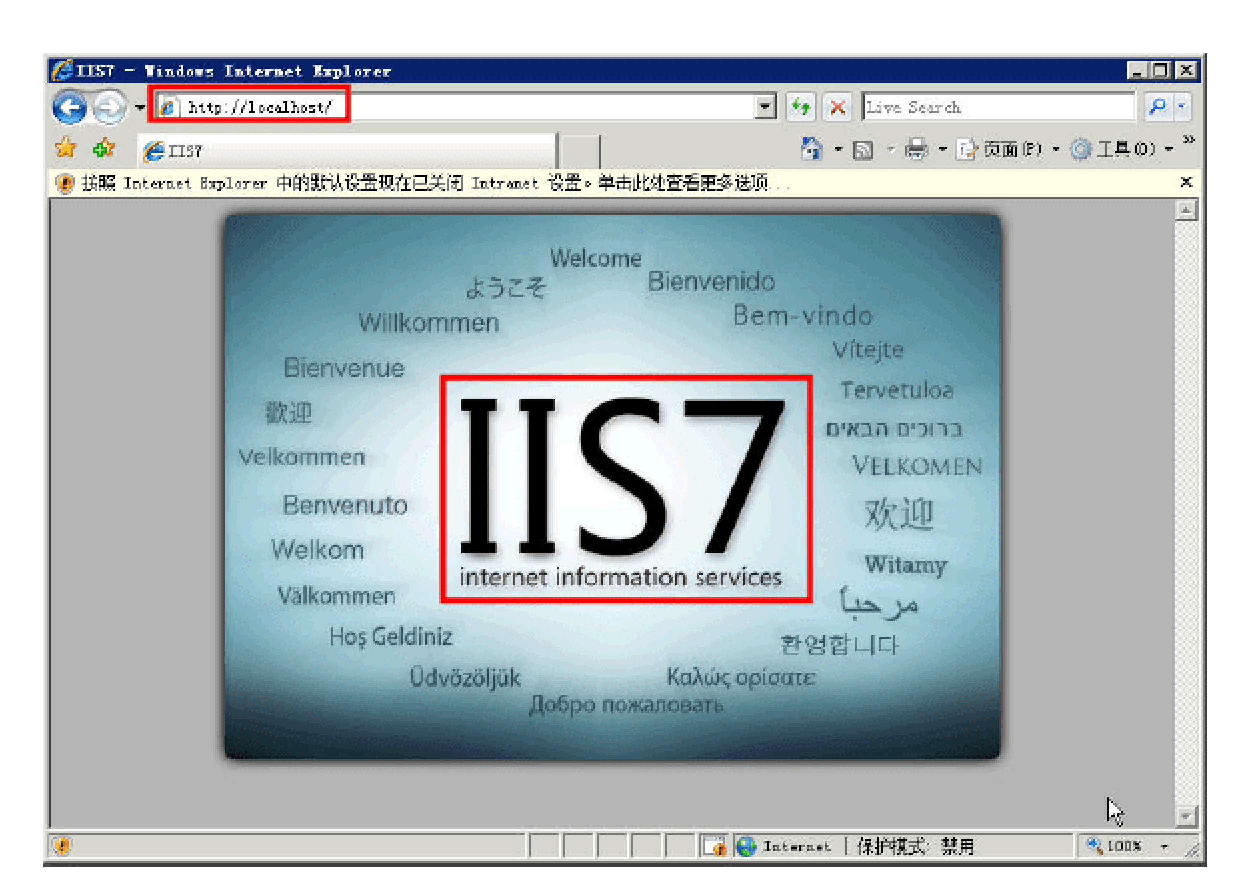


图 5-14　Web 服务器默认主页

安装好 Web 服务器之后，接下来，我们将通过具体的实例介绍 Web 服务器的配置与管理，主

要内容包括：

（1）在一台服务器上创建多个网站的方法与步骤。

（2）Web 服务器的配置与管理。

（3）FTP 服务器的配置与管理。

下面将一一介绍。

5.3　在一台服务器上创建多个网站

在一台服务器上，创建多个网站的方法有以下四种。

（1）IP 地址法：在 Web 服务器上设置多个 IP 地址，每个 IP 地址对应 1 个网站。

（2）端口法：每个 TCP/IP 的地址，可以使用 1～65535 之间的 TCP 端口，每个端口可以对应一个网站。通常来说，在使用“端口法”时，推荐的端口在 1024～65535 之间。

（3）主机头法：采用 DNS 名称的方法，每个网站采用一个不同的主机头。

（4）虚拟目录法：通过创建虚拟目录的方法，创建多个网站。严格来说，虚拟目录是依赖于一个或多个网站，不能算独立的网站。

如果 Web 服务器主要应用于局域网，一般多采用 IP 地址法、端口法，或者两者的组合创建多个网站，如果 Web 服务器主要用于 Internet 网络，通常采用主机头法。当然，具体采用哪种方法，或者综合使用几种方法，由管理员根据实际情况选择。

接下来，将通过表 5-1 的实例，介绍这几种方法。

表 5-1　创建网站详细信息

IP 地址	端口	主机头	网站位置	客户端访问地址
192.168.1.10	80		e:\web1	http://192.168.1.10
192.168.1.11	80		e:\web2	http://192.168.1.11
192.168.1.12	80		e:\web3	http://192.168.1.12
192.168.1.10	8010		e:\web4-8010	http://192.168.1.10:8010
192.168.1.10	8011		e:\web5-8011	http://192.168.1.10:8011
192.168.1.10	8012		e:\web6-8012	http://192.168.1.10:8012
192.168.1.10	80	www.abc.com	e:\web7-abc.com	http://www.abc.com
192.168.1.10	80	www.xyz.net	e:\web8-xyz.net	http://www.xyz.net
192.168.1.10	80	abc.xyz.cn	e:\web9-abc.xyz	http://abc.xyz.cn
任意 IP	8013	www.abc.com	e:\web10-abc.com	http://www.abc.com:8013

5.3.1　使用 IP 地址法创建 Web 站点

在 IIS 服务器上，如果服务器的“本地连接”中绑定了多个 IP 地址，可以在 IIS 服务器上，通过为不同的网站选择（设置）不同的 IP 地址的方法，来实现多个网站。

01 在服务器上设置三个 IP 地址，分别是 192.168.1.10、192.168.1.11 和 192.168.1.12，如图 5-15 所示。

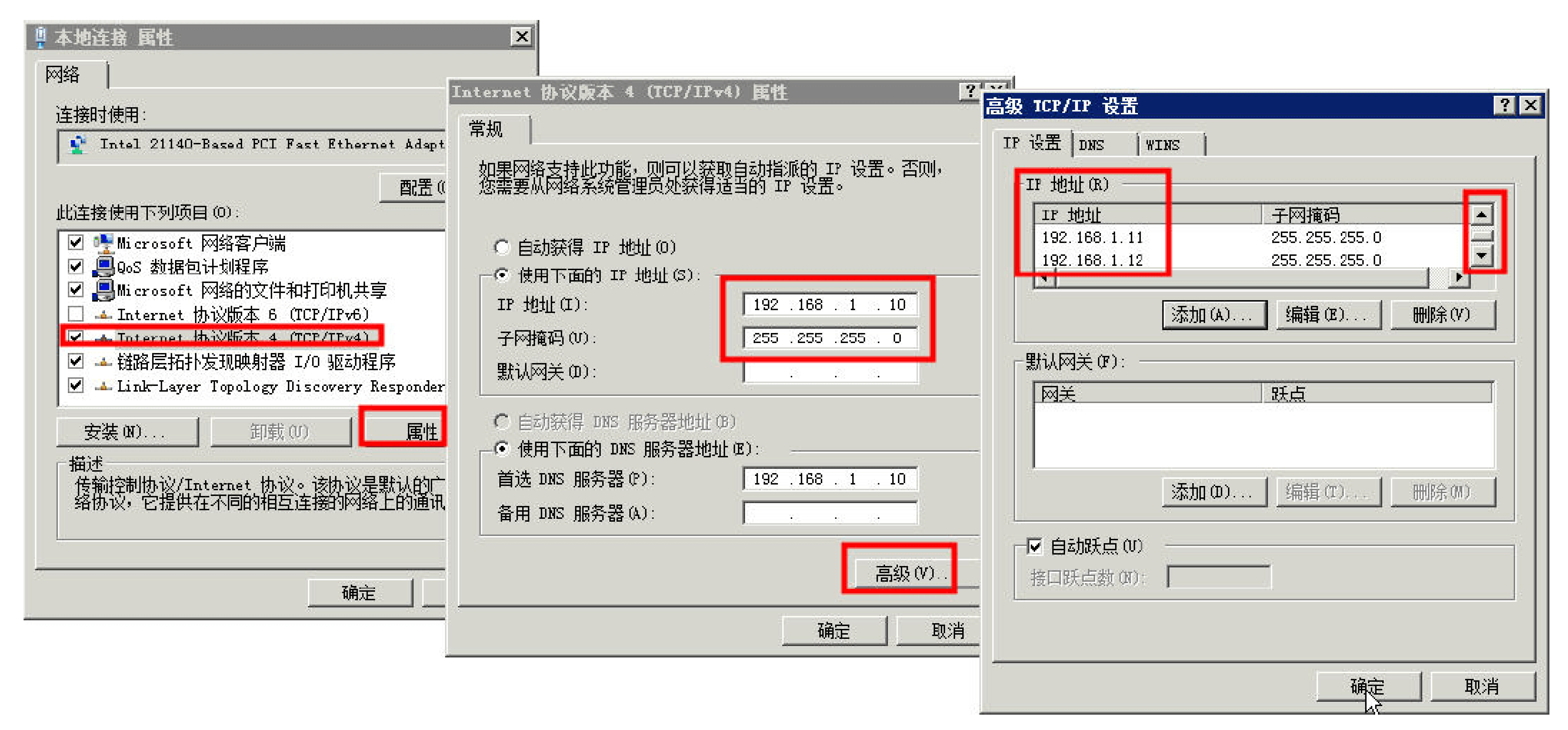


图 5-15　服务器上设置了多个 IP 地址

02 参照表 5-1，在 E 盘创建 10 个目录（如图 5-16 所示），并在每个目录中，新建一个名为 default.htm 的文件，每个文件的内容格式如下：

```
目录名　网站打开地址
```

例如，对于 E:\web1 文件夹中 default.htm 的内容为：

```
E:\WEB1　http://192.168.1.10
```

对于 E:\web10-abc.com 的内容为：

```
E:\WEB1-abc.com　http://www.abc.com:8013
```

可以使用“记事本”在每个目录打开 default.htm 并编辑，如图 5-17、图 5-18、图 5-19 所示。

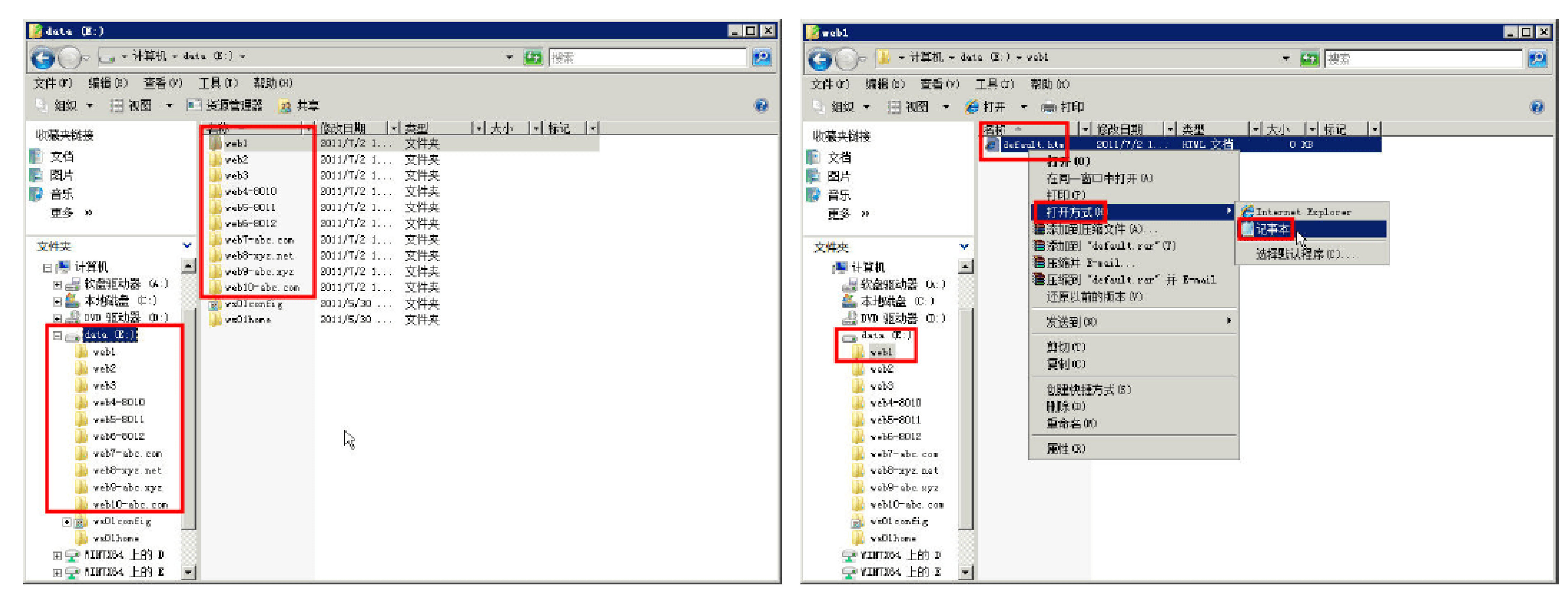


图 5-16　创建文件夹　　　　图 5-17　用“记事本”编辑 default.htm 文件

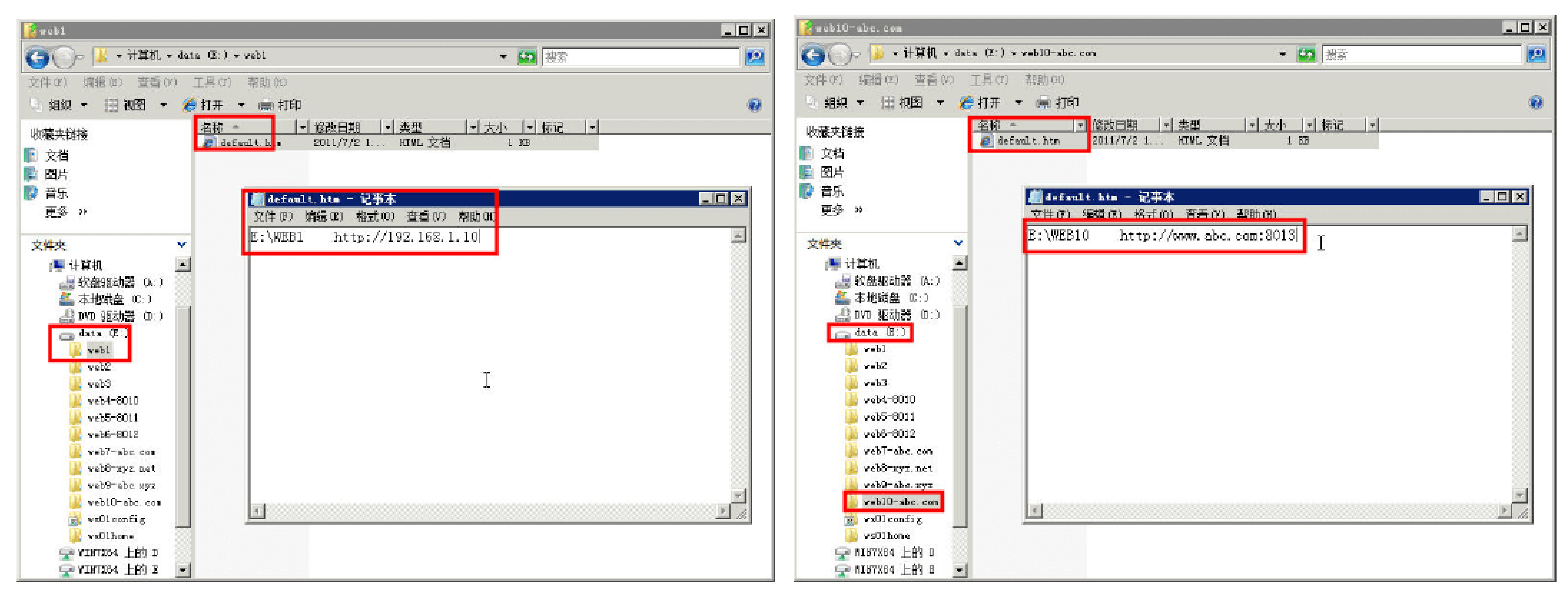


图 5-18　编辑 web1 中的 default.htm 文件　　图 5-19　编辑 web10-abc.com 中的 default.htm 文件

03 从“所有程序→管理工具”中运行“Internet 信息服务（IIS）管理器”，选中“Default Web Site”选项，在右侧的“操作”列表中，单击“停止”命令，将默认网站（图 5-14 显示的内容）停止，如图 5-20 所示。

04 在“网站”窗格中，在空白位置用鼠标右击，在弹出的快捷菜单中选择“添加网站”选项（如图 5-21 所示），或者在“操作”窗格单击“添加网站”链接，都将打开新建网站对话框。

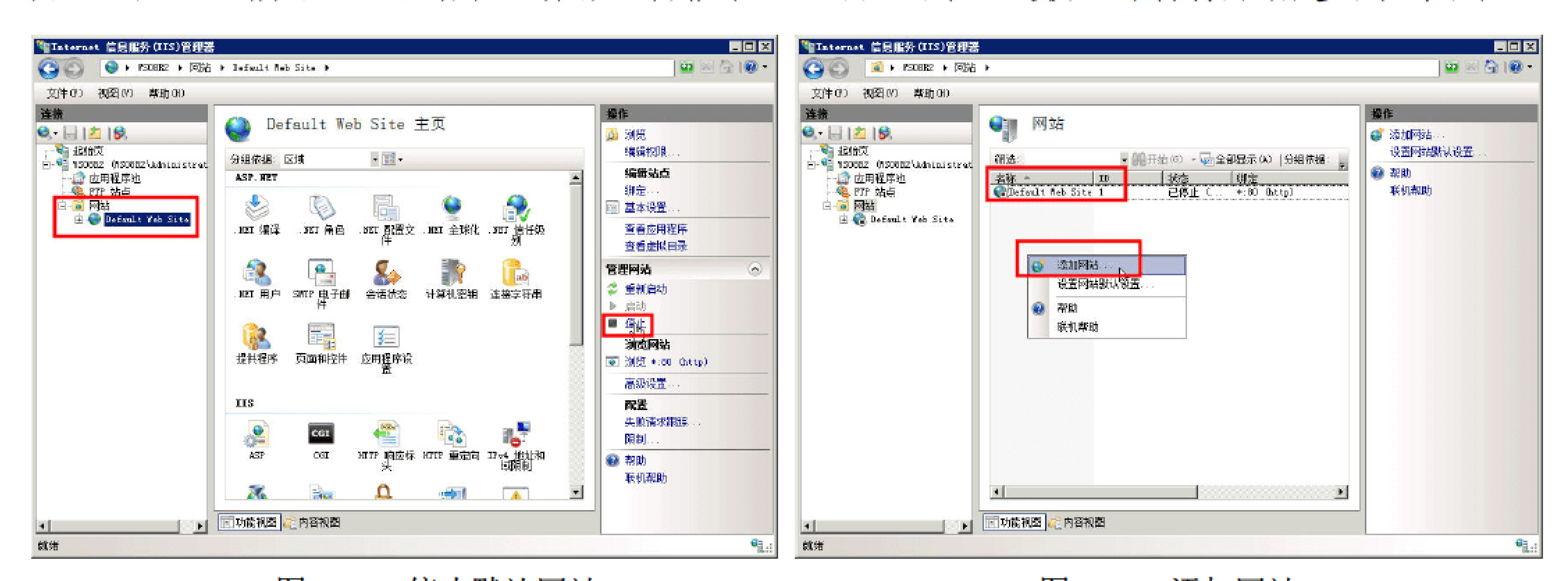


图 5-20　停止默认网站　　图 5-21　添加网站

05 在弹出的“添加网站”对话框中，在“网站名称”文本框中，输入将要添加的网站的名称，在“物理路径”处选择将要添加的网站的位置，在“IP 地址”下拉列表中，选择要添加的网站绑定的 IP 地址，在“端口”文本框中，指定网站所绑定的端口（默认为 80），在“主机头名”文本框中，输入将要创建的网站的主机名。在本例中，参照图 5-21，添加用于 IP 地址的网站，首先创建第 1 个网站，IP 地址为 192.168.1.10、网站路径为 e:\web2，如图 5-22 所示。设置好之后，单击“确定”按钮，创建第 1 个网站。

06 然后参照图 5-22 的步骤，创建第 2、第 3 个网站。

07 使用这种方法创建的网站，在客户端的浏览器上，通过 http://ip 的方式就可以访问网站，用户可以分别用 http://192.168.1.10、http://192.168.1.11、http://192.168.1.12 访问网站，如图 5-23 所示。

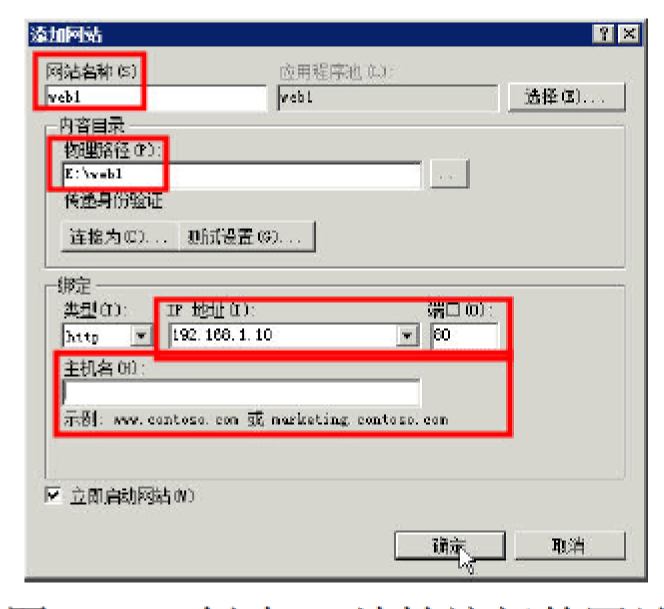


图 5-22　创建 IP 地址访问的网站

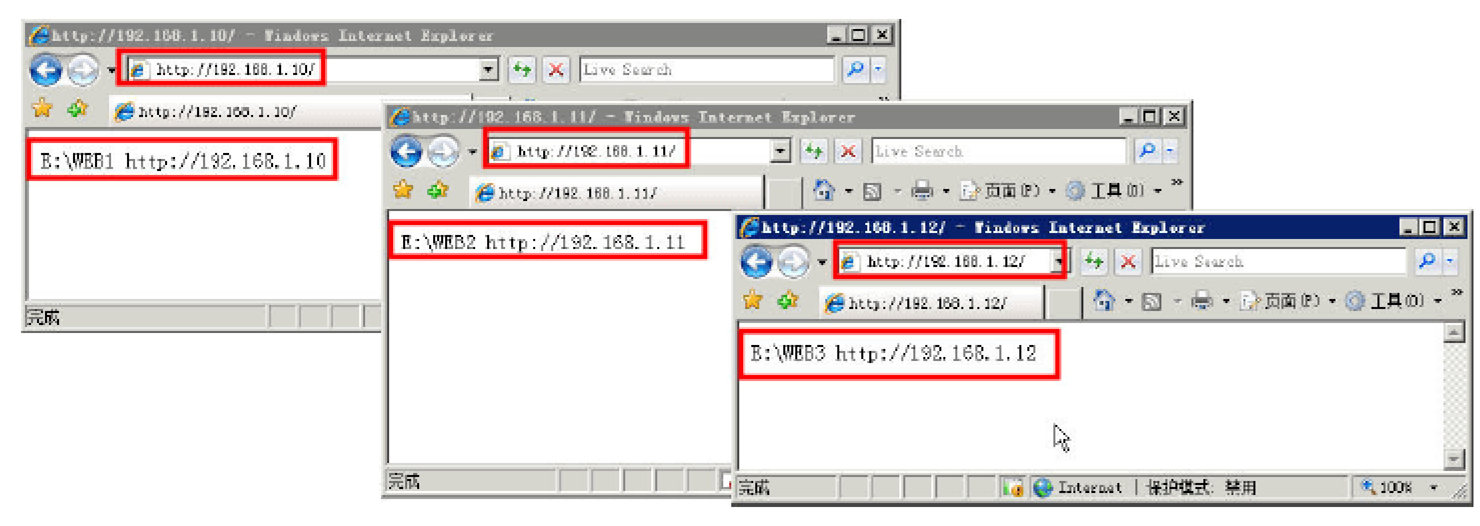


图 5-23　测试三个网站

5.3.2　使用端口法创建 Web 站点

在安装 IIS 时，创建的第一个网站（默认网站）将使用 TCP 的 80 端口。实际上，还可以使用其他端口（通常为 1024~65535 数值）。下面来介绍，怎样用端口法访问这些网站。

参照 5.3.1 节第 4 步的作法，创建网站，不同之处如下（以创建第 4、第 5、第 6 个网站为例）。

01 在“网站名称”处设置网站名为 web4-8010，物理路径选择 E:\web4-8010，在 IP 地址处选择 192.168.1.10，端口处设置 8010，如图 5-24 所示。设置完成后，单击“确定”按钮。



图 5-24　以端口法创建网站

02 对于第 5、第 6 个网站，可以参照上一步骤设置。

03 使用这种方法创建的网站，在地址栏中使用“http://服务器 IP 地址：端口”访问对应的网站，用户可以使用 http://192.168.1.10:8010、http://192.168.1.10:8011、http://192.168.1.10:8012 浏览创建的第 4、第 5、第 6 个网站，如图 5-25 所示。

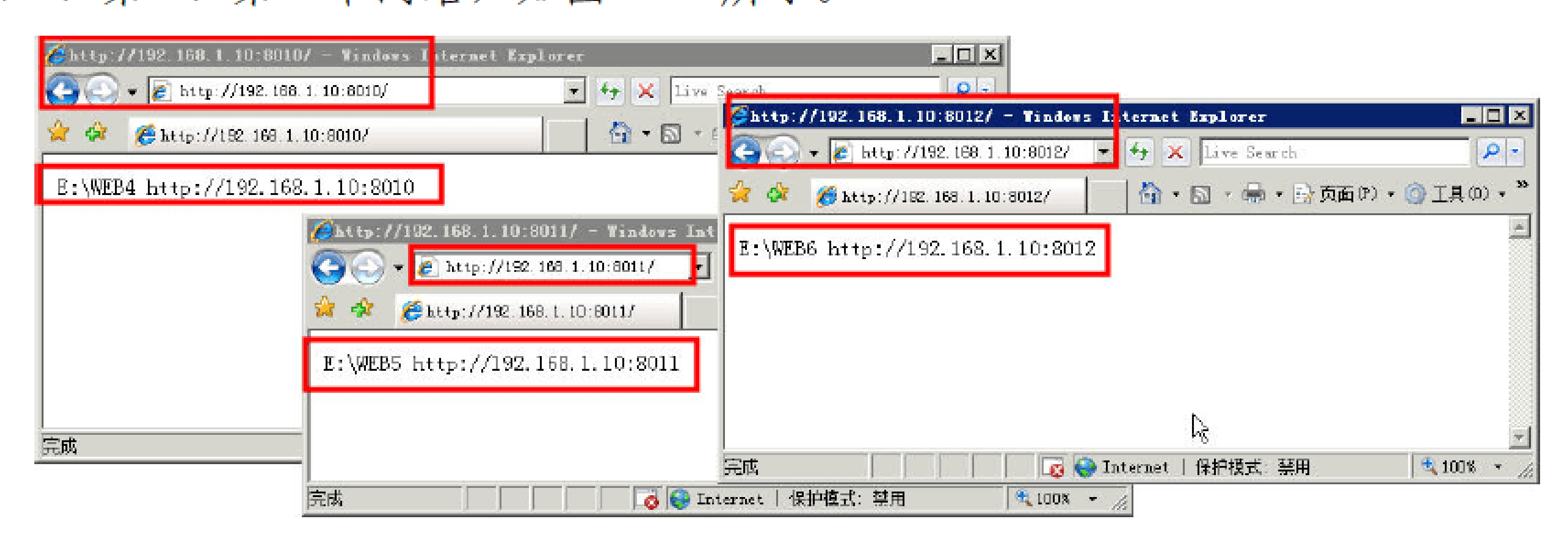


图 5-25　浏览端口法创建的网站

5.3.3 使用主机头名创建 Web 站点

实际上，目前创建 Web 站点使用最多的就是“主机头名”法。对于提供服务器托管的公司，也只有一个合法的 IP 地址，在一个服务器上放置多个不同域名的网站，就是使用“主机头名”法保存多个 Web 站点。

以主机头名法创建网站，与使用 IP 地址、端口法创建网站相似，只是需要在“主机名”中，指定创建网站的“主机名（通常为对外显示的 DNS 名称）”即可，下面以创建第 7、第 8、第 9、第 10 个网站为例进行介绍。

01 打开“添加网站”对话框，在“网站名称”中，输入 web7-www.abc.com，设置物理路径为 E:\web7-abc.com，在 IP 地址处，选择该网站要绑定的 IP 地址，如果选择“全部未分配”表示可以使用该服务器上的每个 IP 地址，然后在主机名处输入 www.abc.com，如图 5-26 所示。设置完成后，单击“确定”按钮，添加网站。

02 然后参照上述步骤，创建第 8、第 9 个网站。

03 在创建第 10 个网站时，指定端口为 8013，主机名为 www.abc.com，如图 5-27 所示。

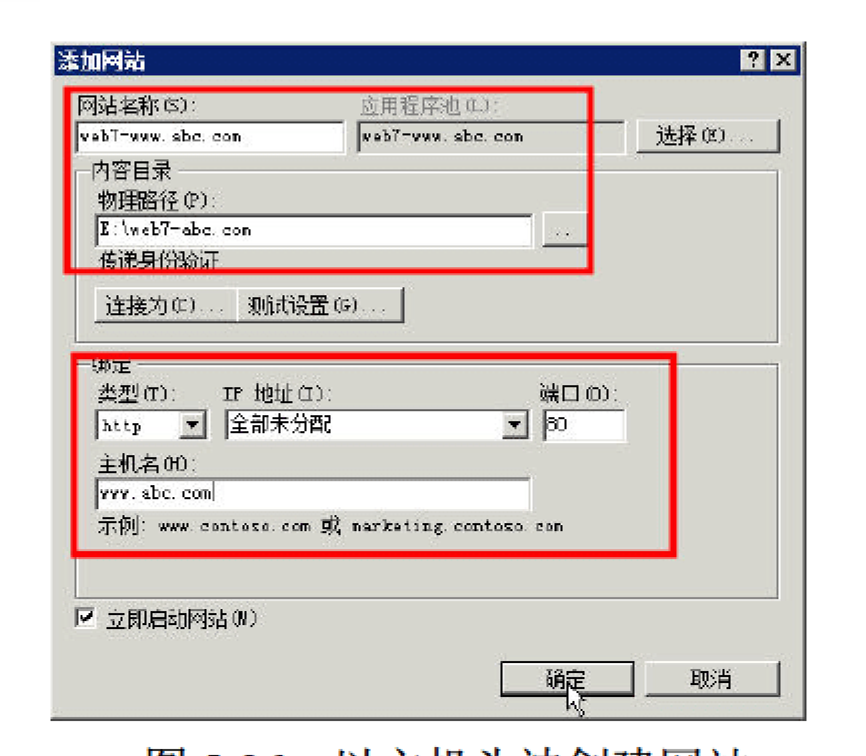


图 5-26　以主机头法创建网站

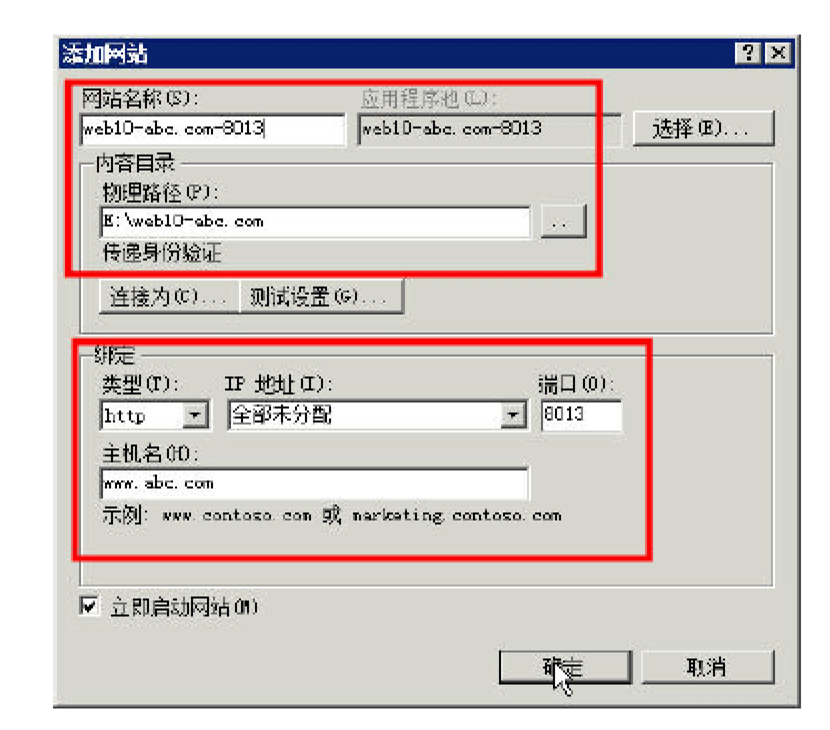


图 5-27　创建第 10 个网站

04 在创建完网站之后，可以看到，如果网站的状态没有更新，可以在左侧窗格中用鼠标右击，在弹出的快捷菜单中选择“刷新”（如图 5-28 所示），在刷新之后，就可以看到网站更新后的状态，如图 5-29 所示。

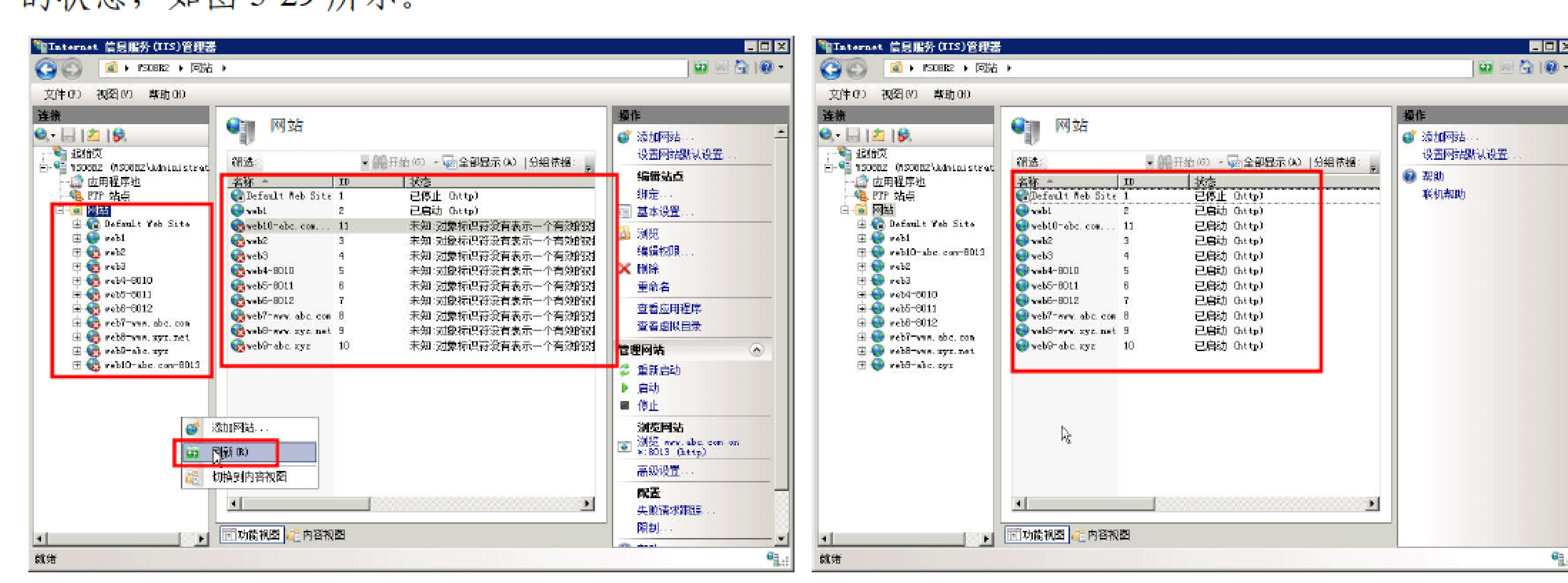


图 5-28　刷新网站　　　图 5-29　刷新网站后的状态

在使用“主机头”法创建网站之后，如果要测试，需要将 www.abc.com 等名称，解析成对应的网站的 IP 地址，我们可以通过编辑测试端的 hosts 文件，浏览测试这些网站，步骤如下。

01 在“运行”地址中输入 c:\windows\system32\drivers\etc\hosts，如图 5-30 所示。

02 在弹出的“打开方式”对话框中选择“记事本”，如图 5-31 所示。

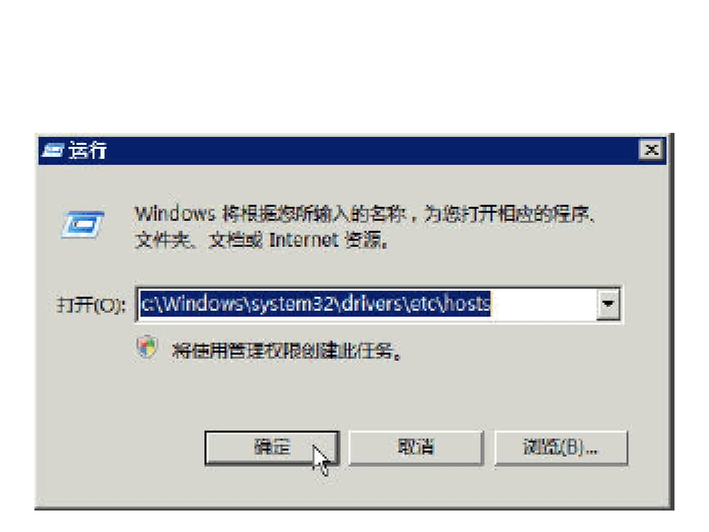



图 5-30　编辑 hosts 文件

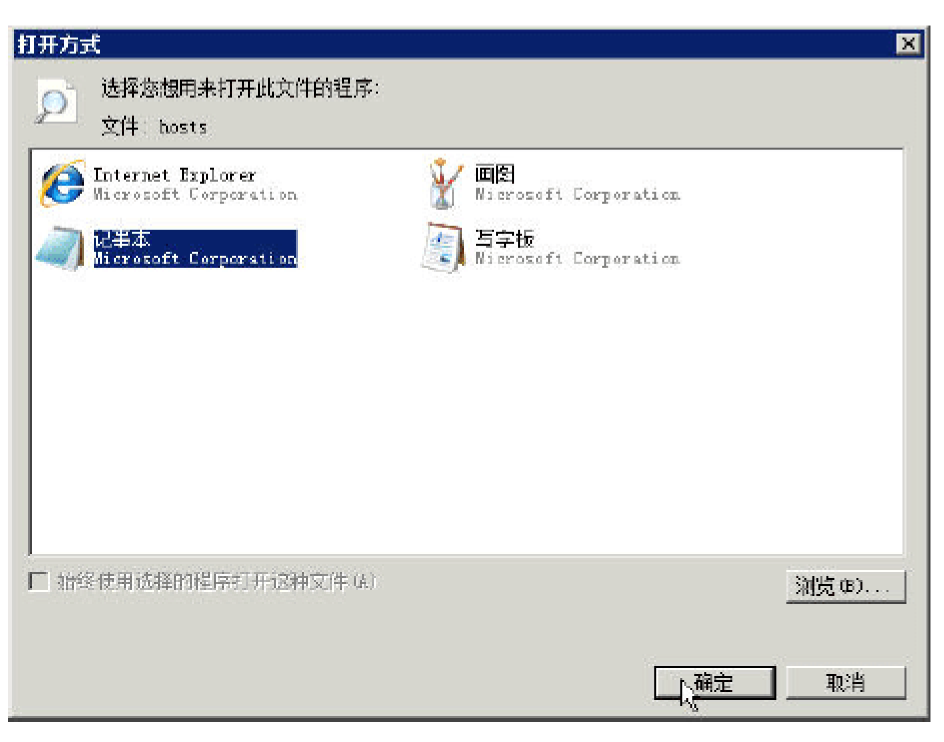


图 5-31　用记事本打开 hosts 文件

03 打开之后，添加 www.abc.com、www.xyz.net、abc.xyz.cn 到 192.168.1.10 的解析，如图 5-32 所示，然后保存退出。

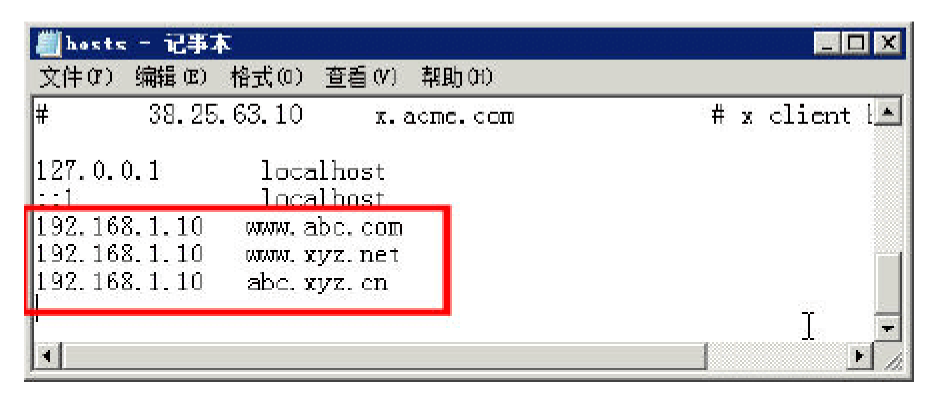


图 5-32　编辑并保存 hosts 文件

04 打开 IE 浏览器，测试 http://www.abc.com、http://www.xyz.net、http://abc.xyz.cn 网站，如图 5-33 所示。

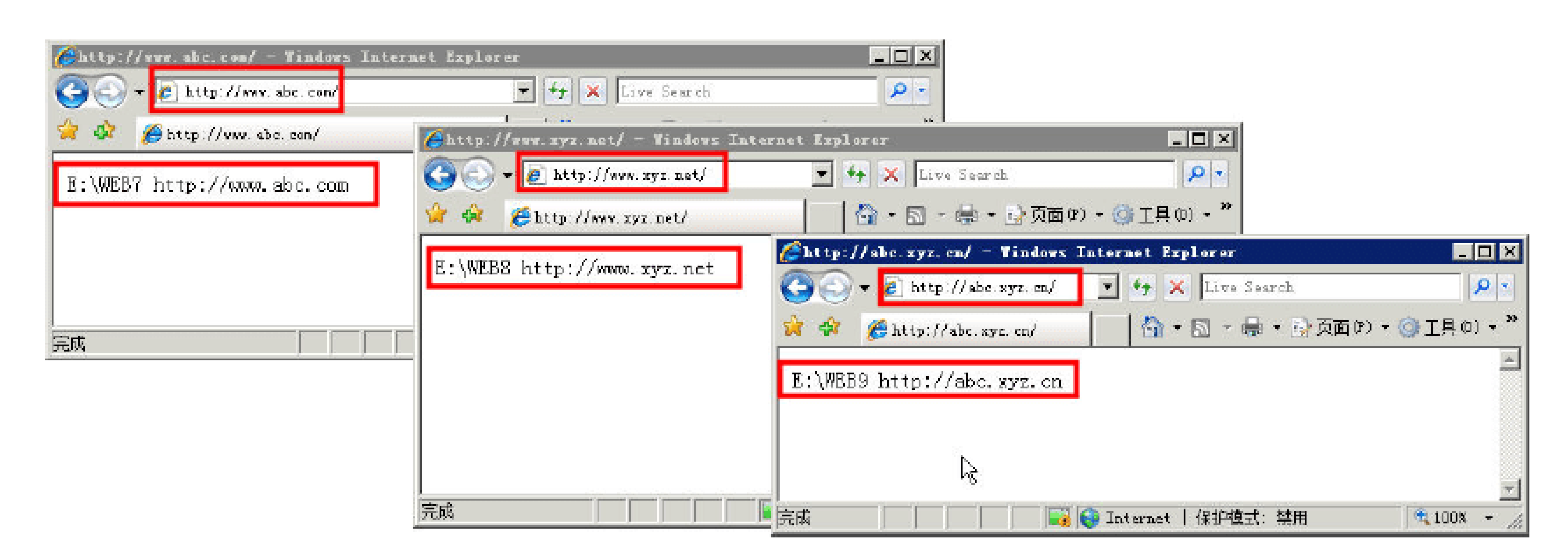


图 5-33　以主机名法测试网站

05 最后，打开 IE 浏览器，测试 http://www.abc.com:8013 网站，如图 5-34 所示。

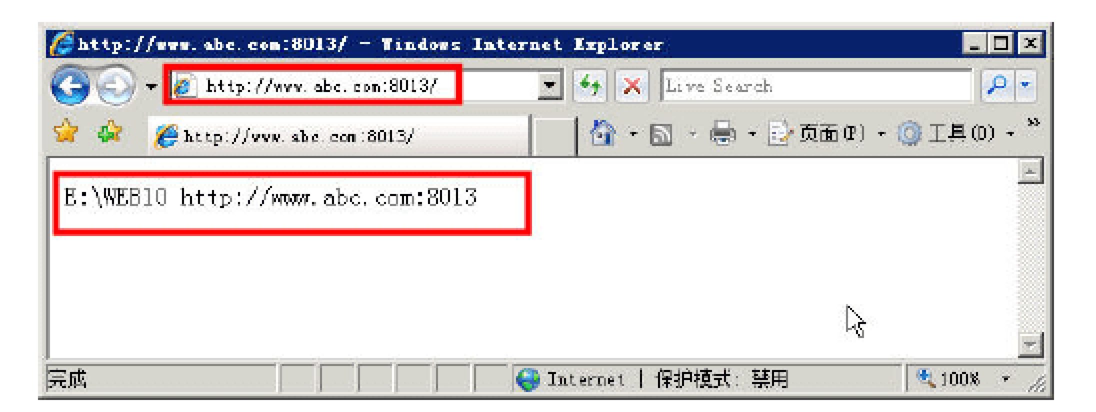


图 5-34　以主机名、端口法测试网站

5.4　管理 Web 服务器

在掌握了如何创建网站之后，接下来，介绍 Web 服务器中每个网站更加详细的配置。我们以前几节创建的网站为例进行介绍。

5.4.1　Web 服务器总体配置

打开“Internet 信息服务（IIS）管理器”，在左侧的任务窗格中，选择一个创建的网站，例如 web10-abc.com-8013，在中间与右侧的窗格显示了网站的所有配置，如图 5-35 所示。

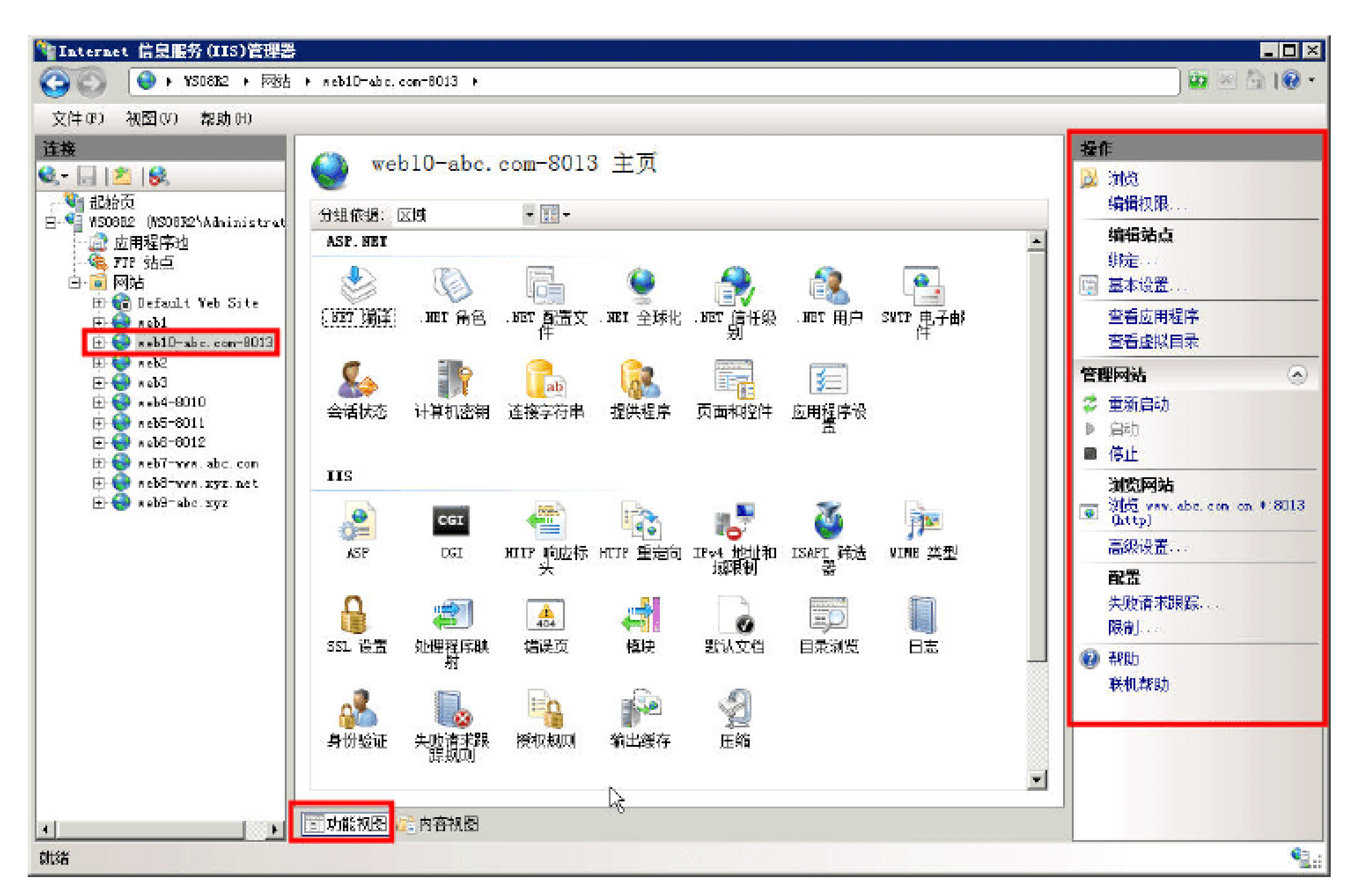


图 5-35　网站配置

在图 5-35 的“中间”窗格，默认显示的是“功能视图”，包括“ASP.NET”、“IIS”、“管理”三大部分，在 IIS 选项中，用户主要用到的功能有：HTTP 重定向、IPv4 地址和域限制、MIME 类型、SSL 设置、错误页、默认文档、目录浏览、身份验证等。在右侧的窗格中包括：浏览、编辑权限、绑定、基本设置、管理网站、浏览网站、配置等。部分功能在后文中将会详细介绍。
在图 5-35 中，单击“内容视图”，可以显示网站中的内容，如图 5-36 所示。

用鼠标右击选中的网站，在快捷菜单中的命令有：浏览、编辑权限、添加应用程序、添加虚拟目录、编辑绑定、管理网站、刷新、删除、重命名等，如图 5-37 所示。这个快捷菜单中的命令，有些与右侧窗格“操作”中的命令相同。

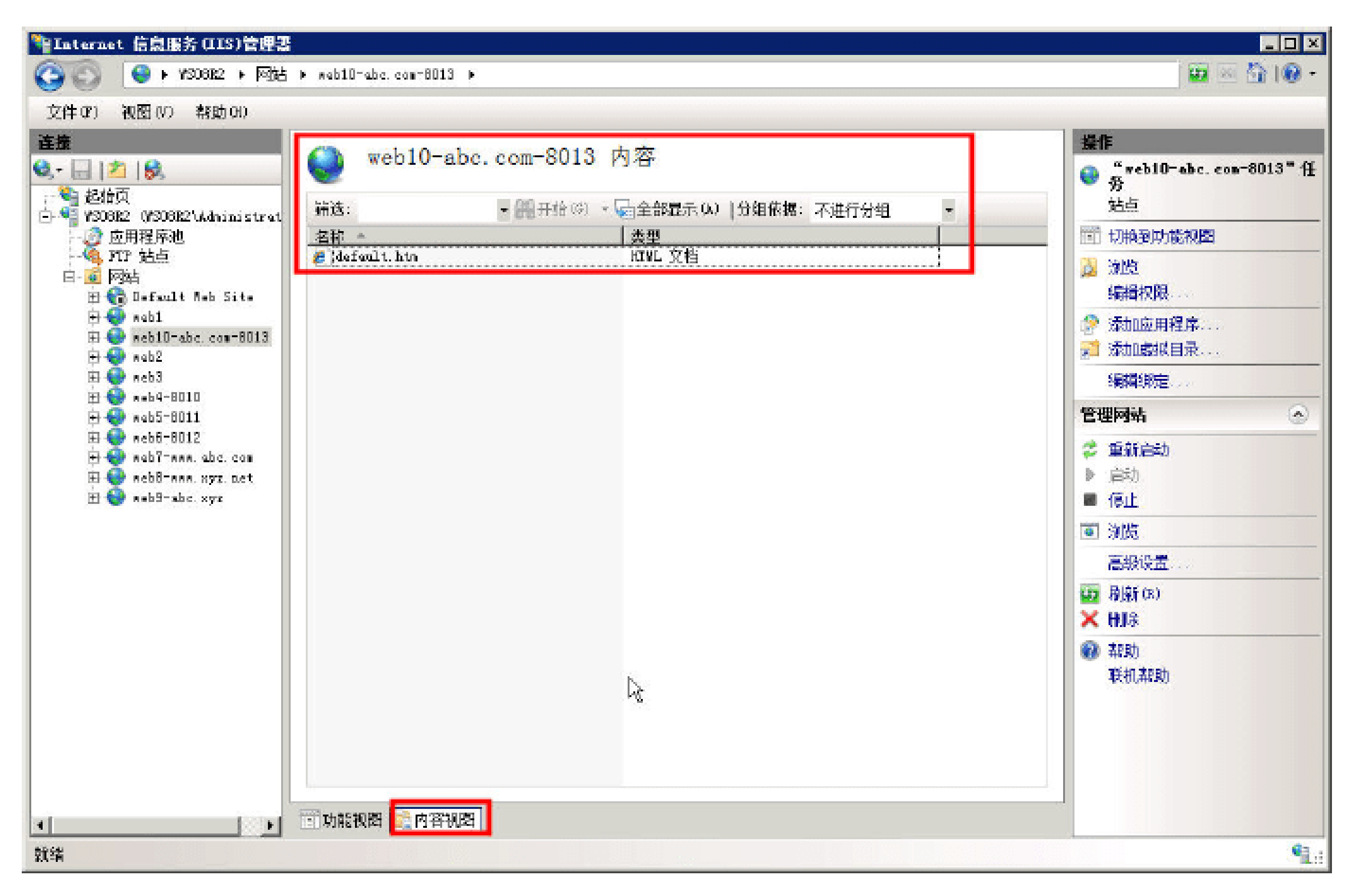


图 5-36　内容视图

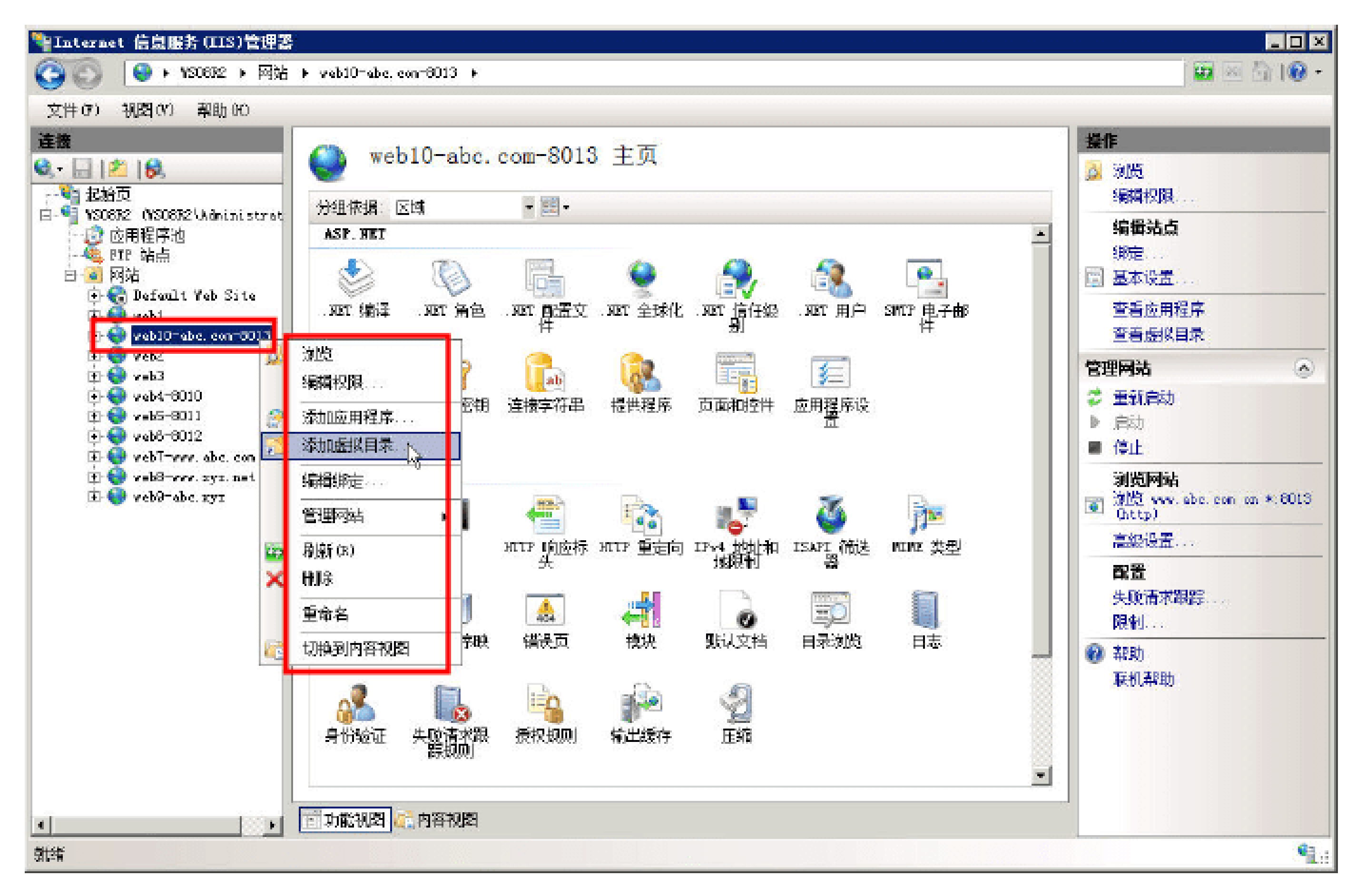


图 5-37　右键快捷命令

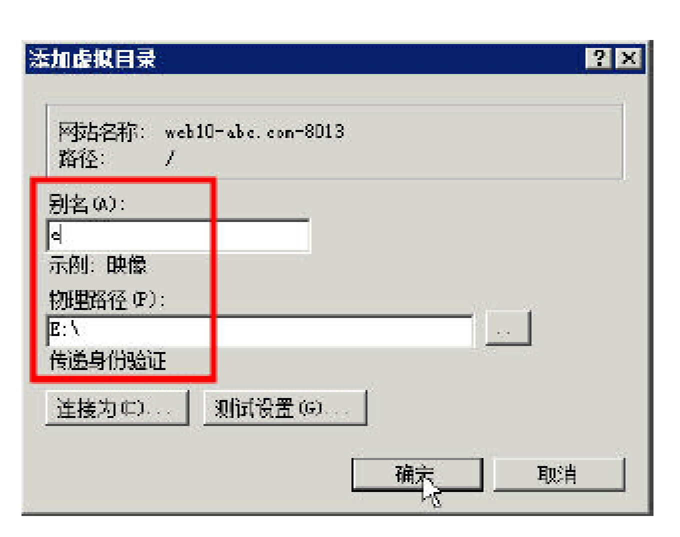
5.4.2　虚拟目录、目录浏览与默认文档

除了可以通过创建网站（IP 地址法、主机头法、端口法）向外展示服务器中的资源外，还可以将资源以“虚拟目录”的方式，添加到网站并对外发布。虚拟目录依赖于网站，像一个网站中的一个文件夹一样。接下来的操作中，将把 E 盘根目录作为一个虚拟目录添加到网站，并为此虚拟目录启用目录浏览功能，步骤如下。

01 用鼠标右击要添加虚拟目录的网站，在弹出的快捷菜单中选择“添加虚拟目录”（如图 5-37 所示），在弹出的“添加虚拟目录”对话框中，在“别名”文本框中，输入要添加的虚拟目录的名称，在“物理路径”中浏览选择要添加的文件夹，如图 5-38 所示，然后单击“确定”按钮，完成添加。

02 在添加完虚拟目录之后，如果要浏览、查看添加的虚拟目录，可以定位到虚拟目录，在图 5-37 右侧的“操作”列表中，单击“浏览 www.abc.com on *:8013”链接，浏览查看虚拟目录。或者直接输入“http://虚拟目录所属网站/虚拟目录名称”的格式，查看虚拟目录。如果添加的虚拟

目录没有“默认文档”，或者没有启用“目录浏览”时，会出现图 5-39 的错误。





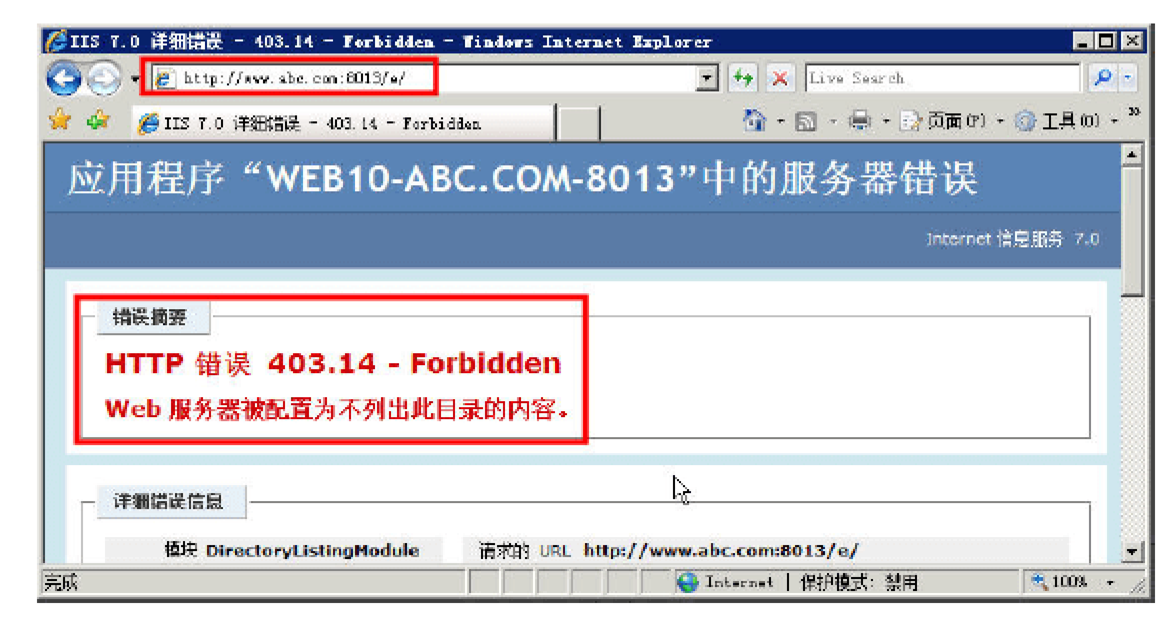


图 5-38　添加虚拟目录　　　　图 5-39　无默认文档并且没有启用目录浏览

03 如果启用目录浏览，或者添加默认文档，将会显示目录的内容或者显示默认文档。在“Internet 信息服务（IIS）管理器”中，定位到虚拟目录，在中间的窗格中，双击“目录浏览”图标，如图 5-40 所示。

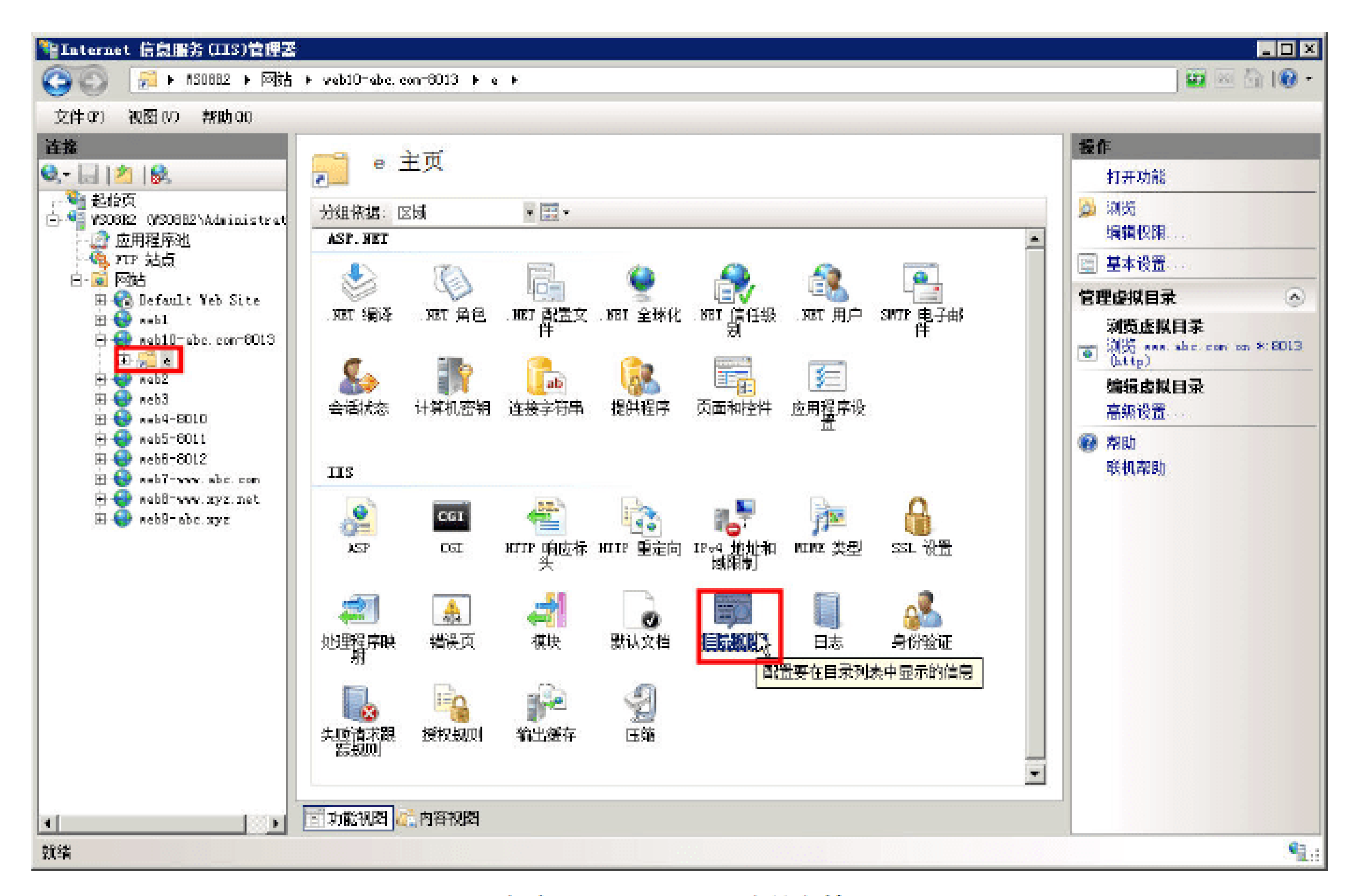


图 5-40　目录浏览

04 在右侧的“警报”窗格中，单击“启用”链接，启用目录浏览，如图 5-41 所示。

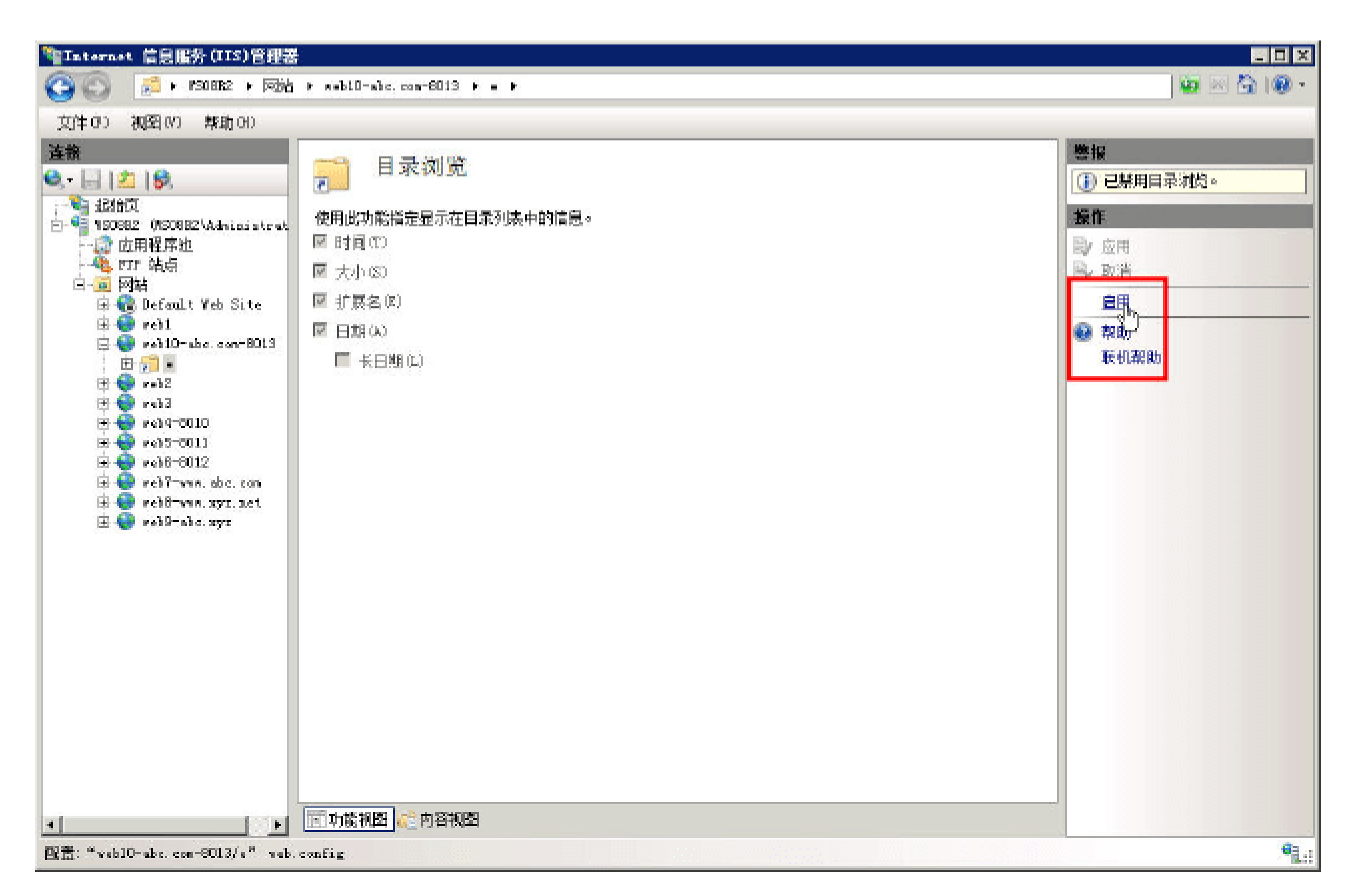


图 5-41　启用目录浏览

05 在启用目录浏览之后，再次浏览查看虚拟目录，将会显示目录的内容，如图 5-42 所示。此时，单击该目录中的某个浏览，将会进入下级目录。如果该目录中有默认文档，将会显示默认文档内容；如果没有默认文档，将会以列目录的方式显示该子目录的内容。

06 切换到图 5-40，双击“默认文档”图标，可以显示默认文档的名称及默认显示顺序，如图 5-43 所示。用户可以选中一个默认文档之后，在右侧的“操作”窗格中，上移、下移文档的顺序，或禁用、删除该默认文档。也可以单击“添加”按钮，添加默认文档。

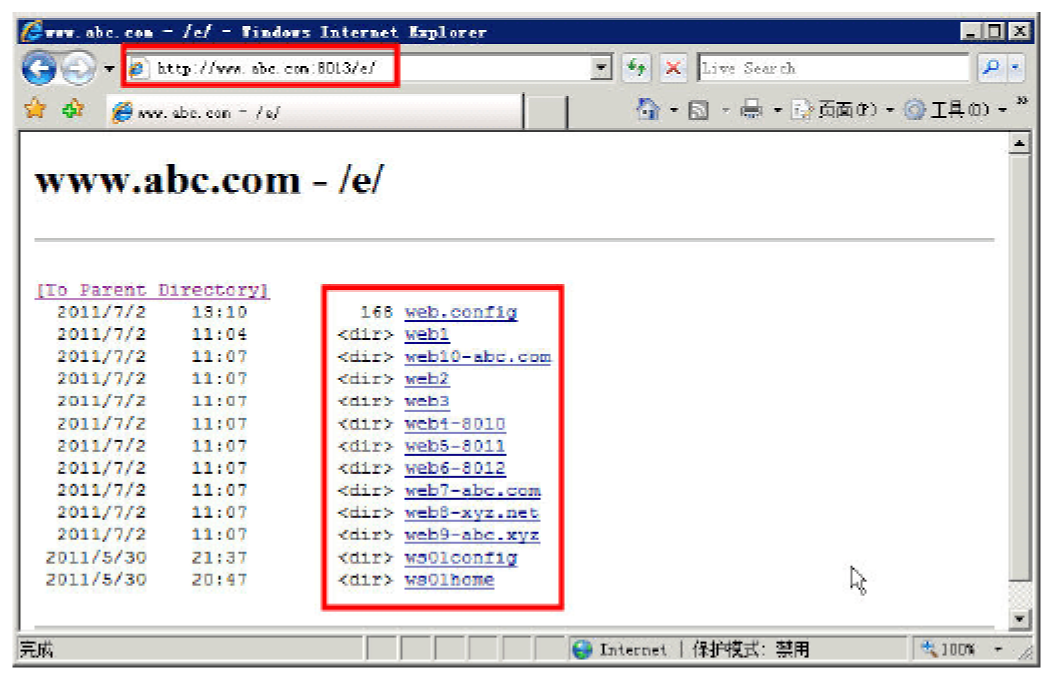


图 5-42 启用目录浏览功能

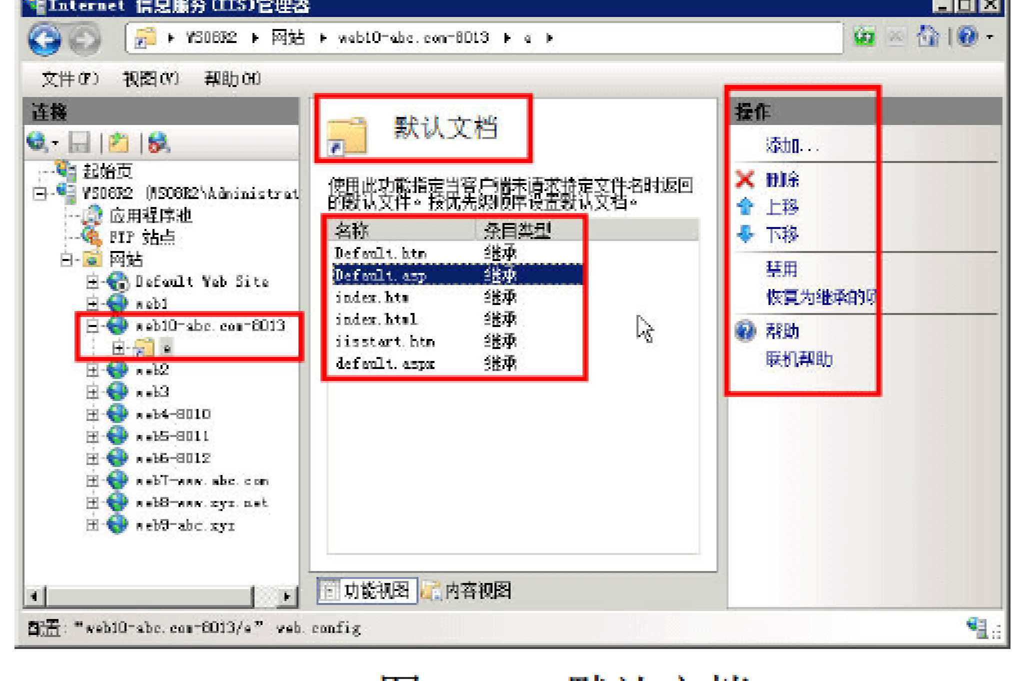


图 5-43 默认文档

07 在图 5-43 中，单击“添加”按钮，在弹出的对话框中，可以添加新的默认文档，例如 abcd.htm，如图 5-44 所示。

08 然后打开“资源管理器”，在 E 盘根目录创建名为 abcd.htm、内容为 e:\ abcd.htm 的文件，重新在浏览器中，浏览查看该虚拟目录，可以看到 abcd.htm 的内容，如图 5-45 所示。

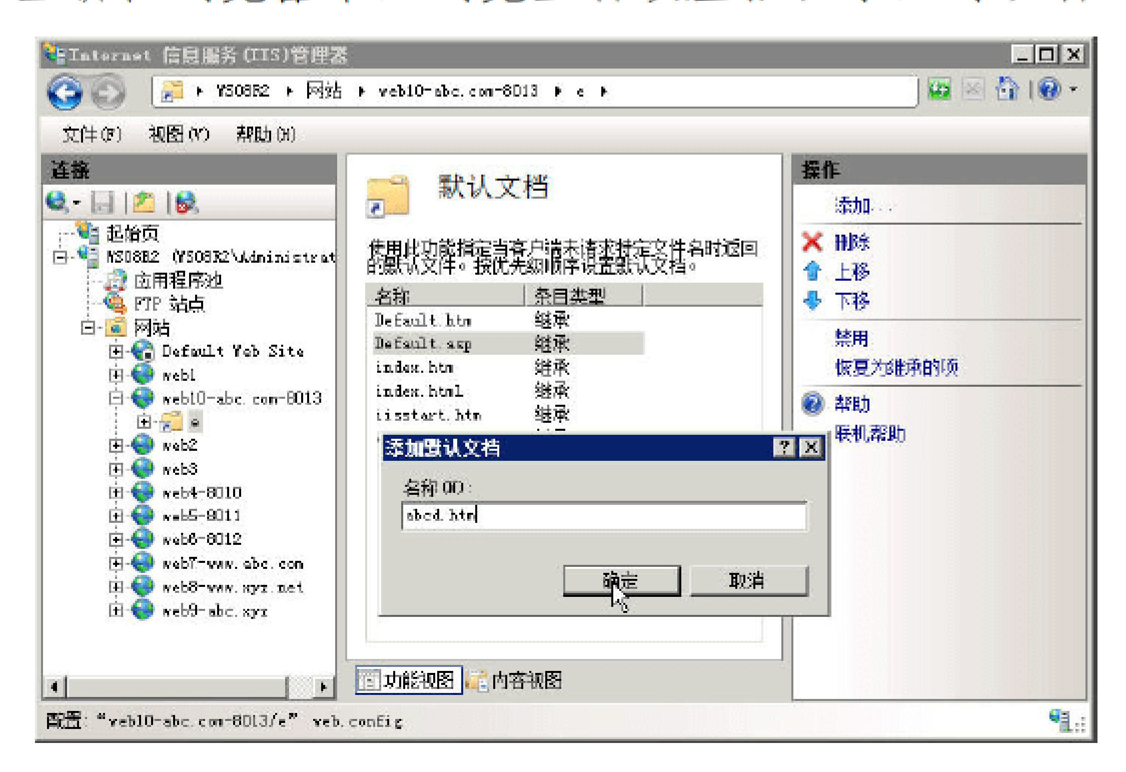


图 5-44 添加名为 abcd.htm 的默认文档

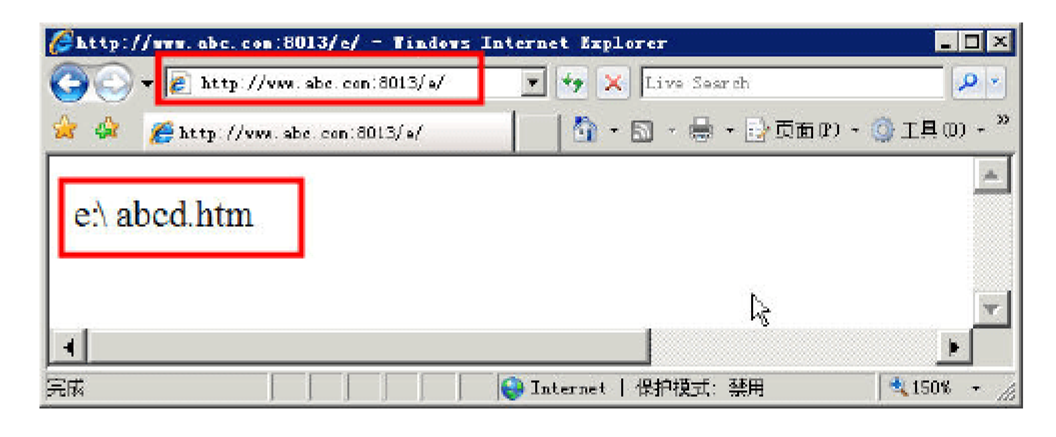


图 5-45 显示默认文档内容

5.4.3 MIME 类型

MIME 是“多用途 Internet 邮件扩展”的简称，使用“MIME 类型”功能页，可以管理 MIME 类型列表，以便能够识别可从 Web 服务器向浏览器或邮件客户端提供的内容的类型。

01 在“Internet 信息服务（IIS）管理器”中，在左侧窗格中，定位到“计算机名”，双击中间的“MIME 类型”图标，如图 5-46 所示。

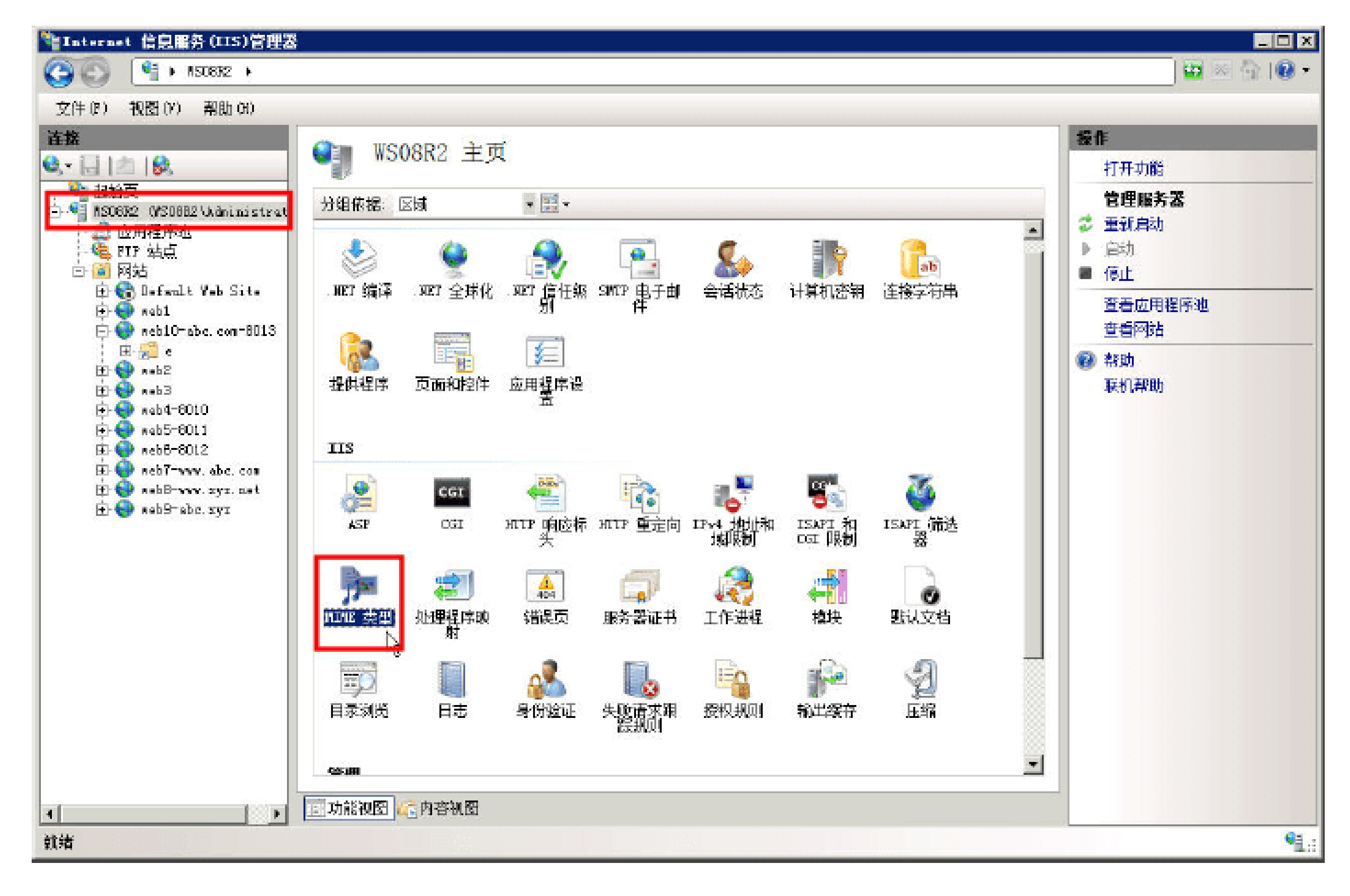


图 5-46　MIME 类型

02 在“MIME 类型”列表中，显示了 IIS 默认支持的 MIME 类型，对于不在该列表中的类型，例如扩展名为 ISO 的文件，当在浏览这些文件（例如提供下载的网站）时，会出现错误。如果要让网站能下载 ISO 的文件（或其他不支持的 MIME 类型文件），用户可以在“MIME 类型”列表中，双击并打开一个现有的 MIME 类型，例如.bin 的 MIME 类型字符串并复制“MIME 类型”文本框中的内容（如图 5-47 所示），然后单击“添加”按钮，添加名为.iso 的类型并“粘贴”复制的 MIME 类型字符串，完成添加，如图 5-48 所示。

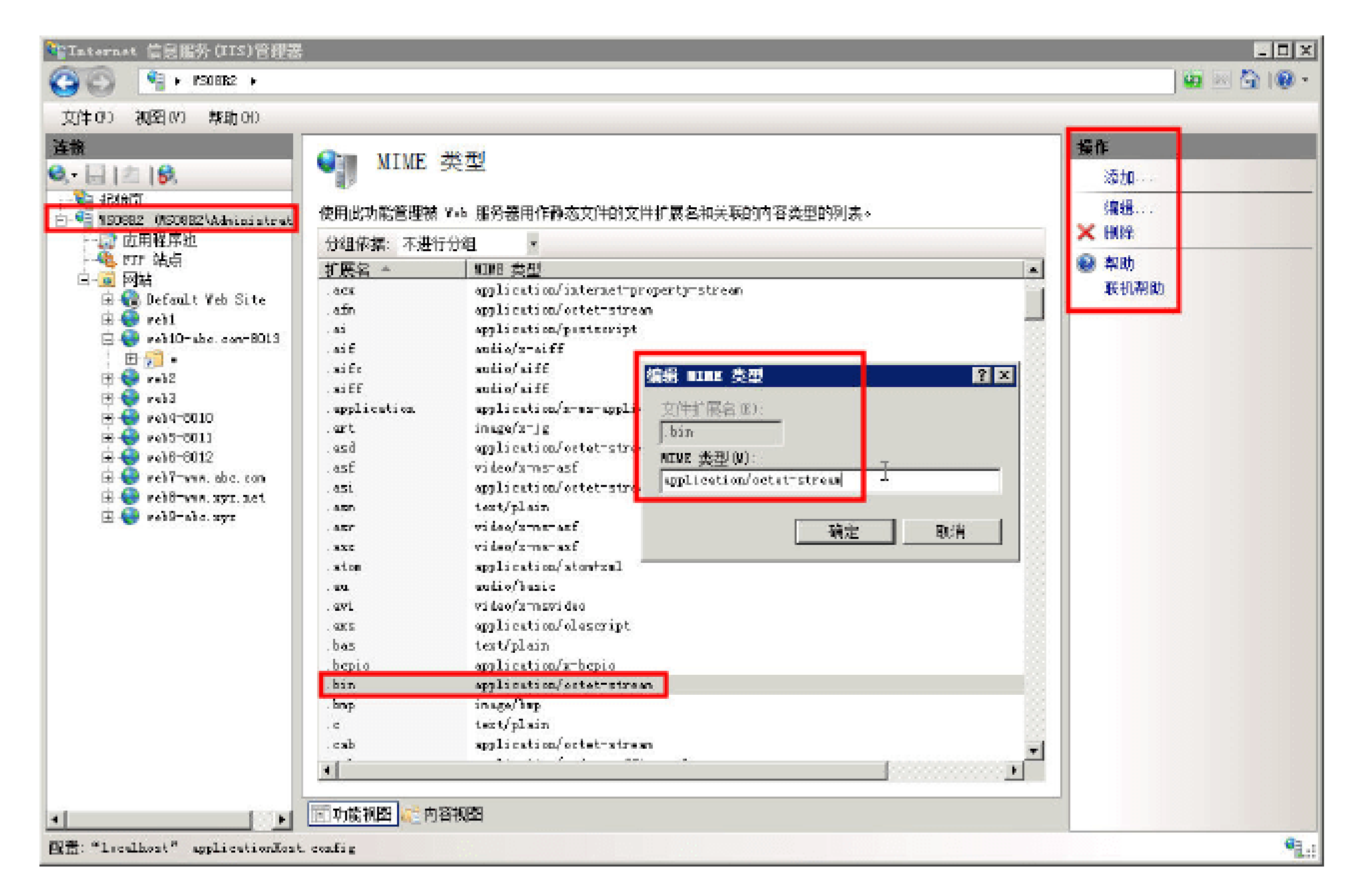


图 5-47　查看并复制现有 MIME 类型



图 5-48　添加名为.iso 的 MIME 类型

5.4.4　HTTP 重定向

使用“HTTP 重定向”功能页可以启用重定向并配置将传入的请求重定向到新目标的方式。例如，在前面的小节中，我们创建并添加了 10 个网站，如果想将用户对 http://192.168.1.12（即 web3 网站）的访问转向到 http://www.abc.com:8013/e，可以按照如下的步骤进行操作。

01 打开“Internet 信息服务（IIS）管理器”，在左侧定位到 web3 网站，在中间双击“HTTP 重定向”，如图 5-49 所示。

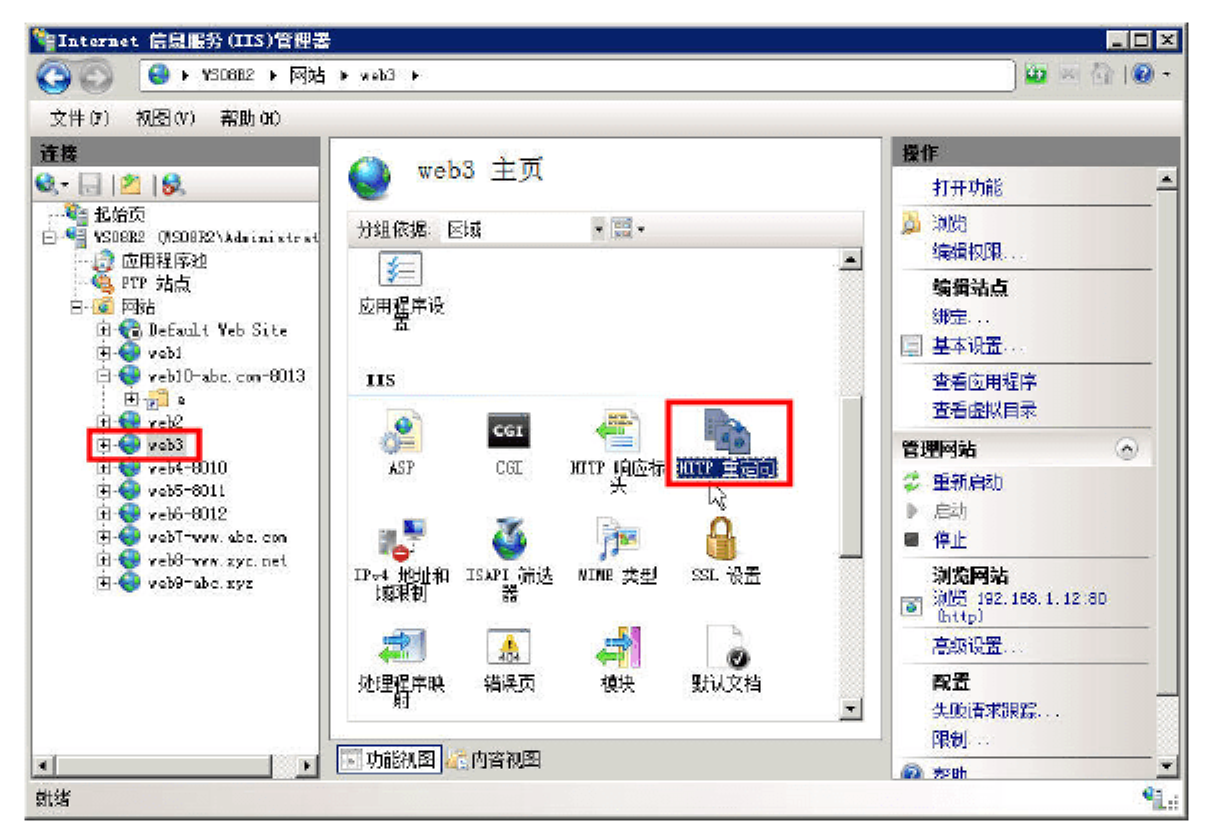


图 5-49　HTTP 重定向

02 在“HTTP 重定向”选项中，选中“将请求重定向到此目标”复选框，然后输入转向到的网站与目录，在本例中为 http://www.abc.com:8013/e，然后单击“应用”按钮，如图 5-50 所示。

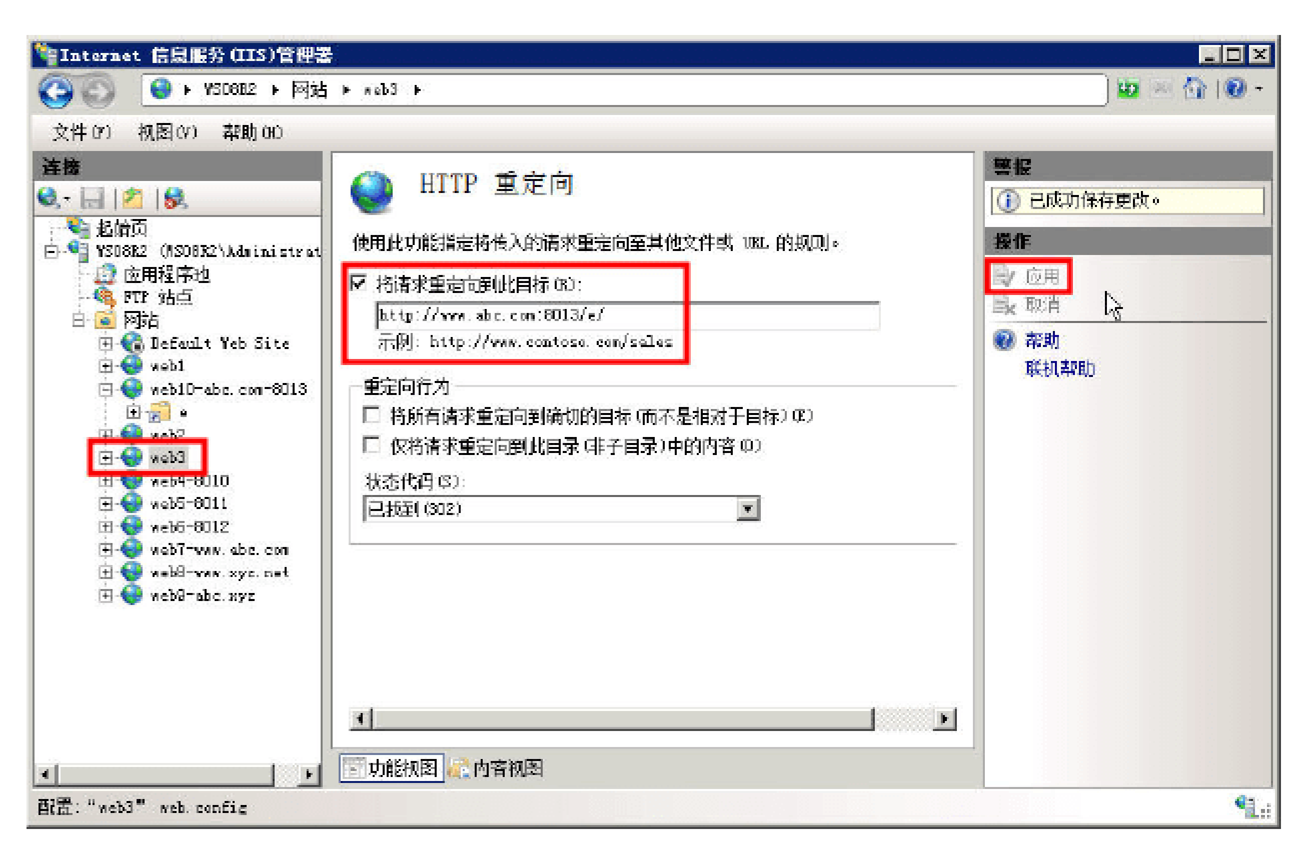
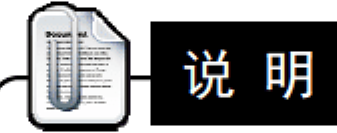


图 5-50　指定重定向网站

以后，当用户访问 http://192.168.1.12 的时候，会被重定向到 http://www.abc.com:8013/e。



说 明

在使用 HTTP 重定向的时候，重定向的目标可以是其他服务器上的其他网站，不一定是当前服务器上存在的网站。

5.4.5　IPv4 地址和域限制

在网站中，可以通过“IPv4 地址和域限制”功能页，允许或拒绝某些 IP 地址浏览访问指定的网站，下面以禁止 192.168.1.0/24 的 IP 地址访问 web3 为例 ，介绍操作步骤。

01 打开“Internet 信息服务（IIS）管理器”，在左侧定位到 web3 网站，在中间双击“IPv4 地址和域限制”图标，如图 5-51 所示。

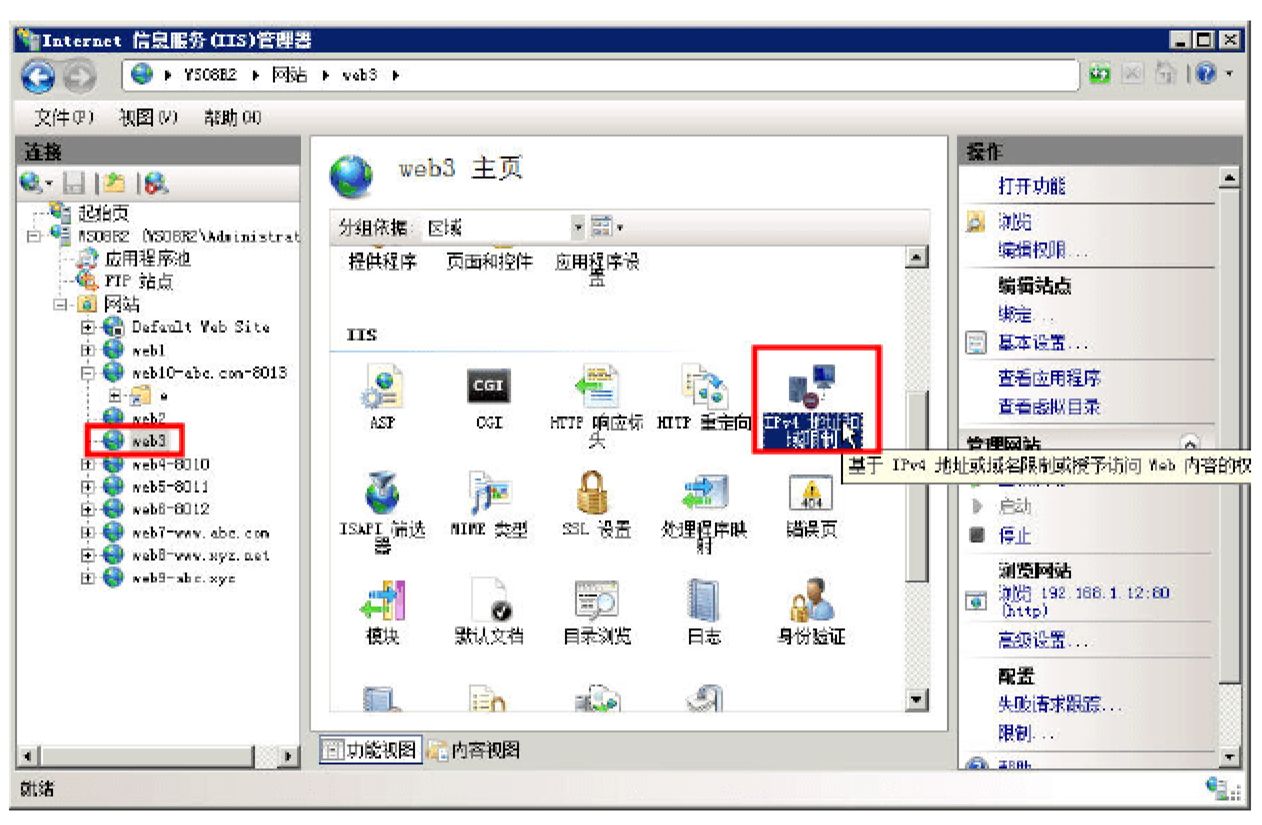


图 5-51　IPv4 地址和域限制

02 在“IPv4 地址和域限制”窗口中，在右侧的“操作”列表中，单击“添加拒绝条目”，选项，在弹出的“添加拒绝限制规则”对话框中，单击“IPv4 地址范围”单选按钮，输入拒绝的地址范围和掩码，如图 5-52 所示。然后单击“确定”按钮。

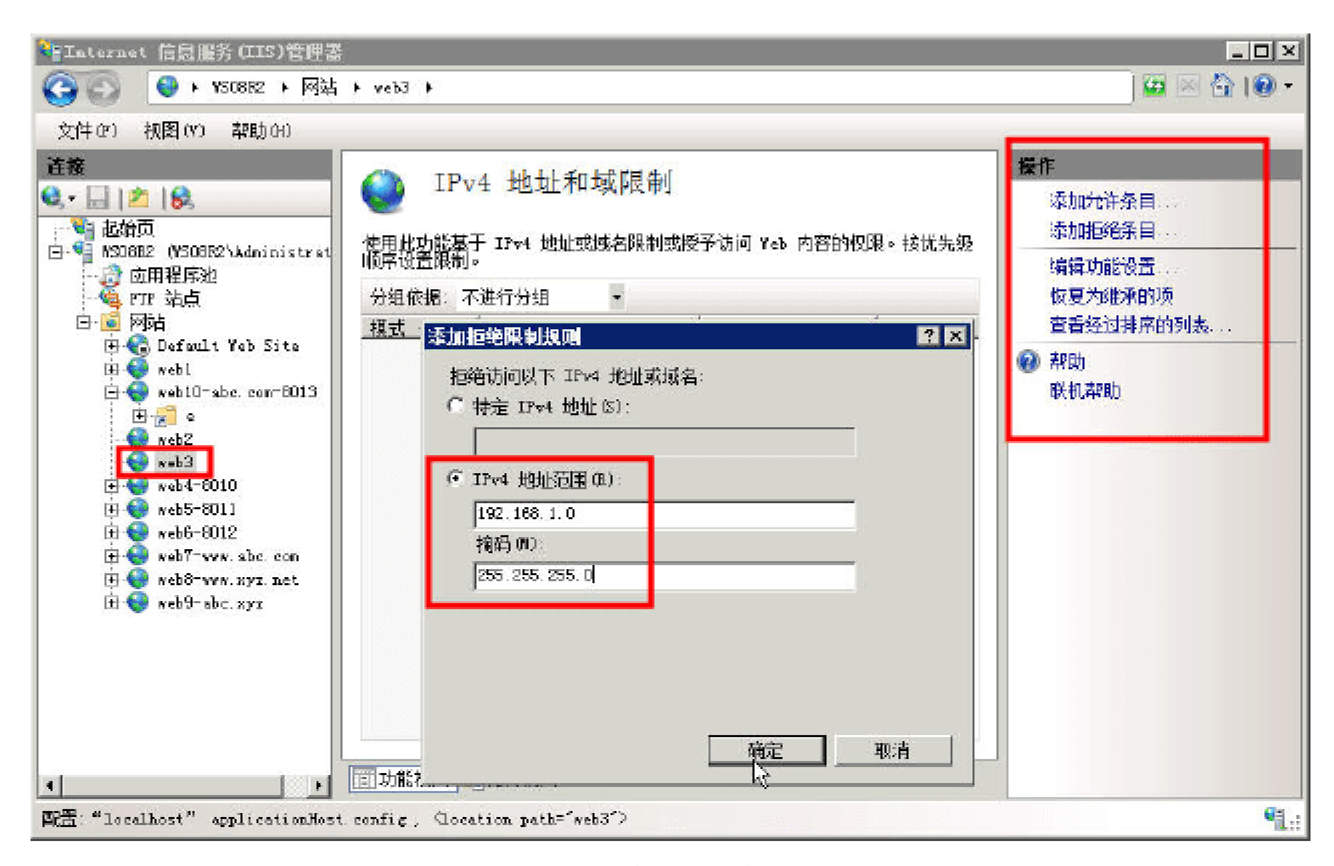


图 5-52　添加拒绝限制规则

在图 5-52 右侧的“操作”窗格中，还可以添加允许条目、编辑功能设置、删除添加的条目等。

03 添加之后，192.168.1.0\24 的 IP 地址在浏览器中浏览 web3（http://192.168.1.12）时会出现错误提示，如图 5-53 所示。



图 5-53　错误 403.6

5.4.6　为网站设置不同的访问方法

无论是使用 IP 地址法创建的网站，还是使用端口法和主机头法创建的网站，这几个网站都是可以“互相转化”的，也可以向一个网站添加多个不同的访问方法。

01 打开“Internet 信息服务（IIS）管理器”，在左侧窗格中定位到 web1 网站，在右侧“操作”列表中单击“绑定”选项，在弹出的“网站绑定”对话框中，添加、删除或编辑（修改）访问方式。例如，可以添加端口为 8888、主机名为 www.abc.com 的访问方式，如图 5-54 所示。

还可以添加多个、其他不同的访问方式，这里不一一介绍。

02 打开 IE 浏览器，浏览 http://www.abc.com:8888，可以看到 web1 的内容，如图 5-55 所示。

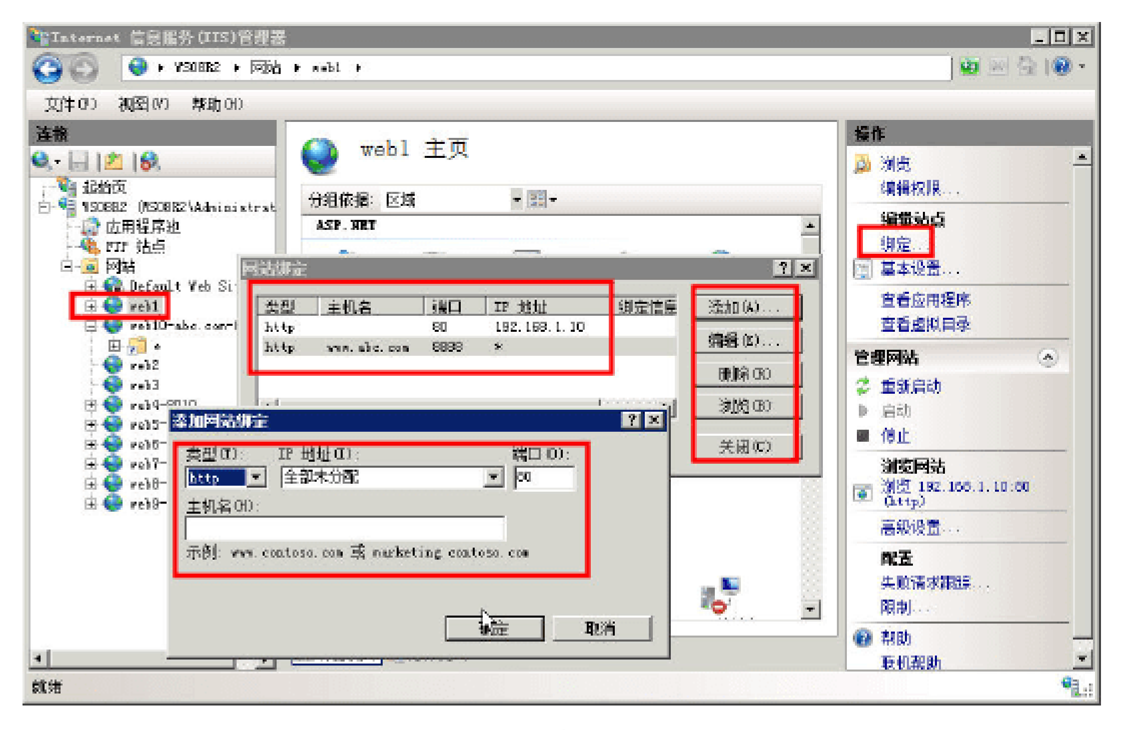


图 5-54　添加新的访问方式

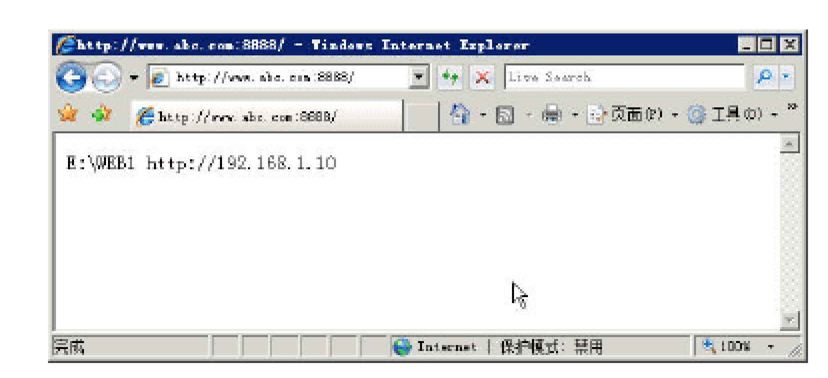
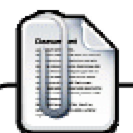


图 5-55　用新的访问方式访问 web1

5.5　配置 FTP 服务器

FTP 是 File Transfer Protocol（文件传输协议）的简称，用于 Internet 上的控制文件的双向传输。同时，它也是一个应用程序（Application）。用户可以通过它把自己的计算机与世界各地所有运行 FTP 协议的服务器相连，访问服务器上的大量程序和信息。FTP 的主要作用，就是让用户连接上一个远程计算机（这些计算机上运行着 FTP 服务器程序）察看远程计算机有哪些文件，然后把文件从远程计算机上拷到本地计算机，或把本地计算机的文件送到远程计算机去。无论是 Linux、还是 Windows，都支持 FTP 服务。在本节介绍 Windows Server 2008、Windows Server 2008 R2 中，FTP 服务器的安装与配置。



说 明

Windows Server 2008 的 FTP 服务器与 Windows Server 2003 的 FTP 服务器相似。而在 Windows Server 2008 R2 中，重新改写了 FTP 服务器的代码，与 Windows Server 2008 的 FTP 服务器有很大的不同。

5.5.1　FTP 服务器概述

FTP 服务器用于上传、下载文件及文件夹，是 Internet 的 3 大基本服务（Web、FTP、E-mail）

之一，在实际工作中有着比较重要的作用。

FTP 的主要作用，就是让用户连接上一个远程计算机（这些计算机上运行着 FTP 服务器程序）察看远程计算机有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件传送到远程计算机上去。

FTP 服务器的工作原理如下：

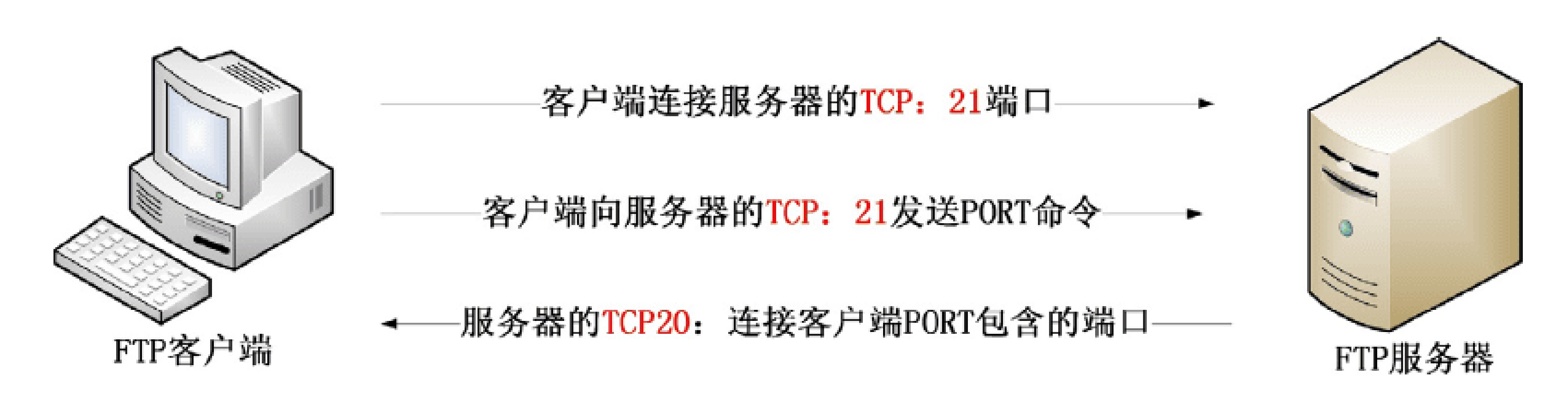
以下传文件为例，当用户启动 FTP 从远程计算机下载文件时，启动了两个程序：一个是本机上的 FTP 客户程序，它向 FTP 服务器提出复制文件的请求。另一个是远程计算机上的 FTP 服务器程序，它响应客户端的请求并把客户端指定的文件发送到客户端计算机中。

在上传文件时，远程计算机的 FTP 服务器接收客户端上传的程序。

FTP 的连接模式有：主动模式（PORT）、被动模式（PASV）。在互联网的所有服务中，FTP 服务器的连接模式是比较复杂的。

1. 主动模式（PORT）

在 FTP 服务器的“主动模式（PORT）”中，FTP 客户端首先和 FTP 服务器的 TCP 21 端口建立连接，通过这个通道发送命令，即客户端需要接收数据的时候在这个通道上发送 PORT 命令。PORT 命令包含了客户端用什么端口接收数据。在传送数据的时候，服务器端通过自己的 TCP 20 端口连接至客户端的指定端口发送数据。 FTP server 必须和客户端建立一个新的连接用来传送数据，如图 5-56 所示。



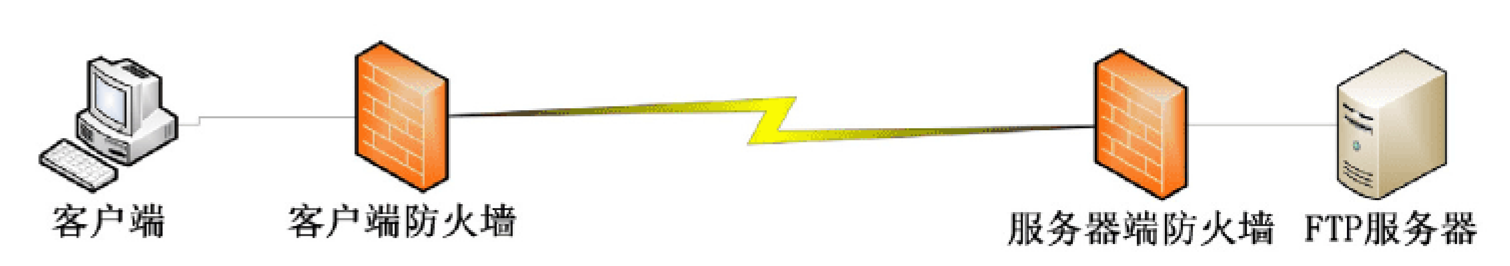
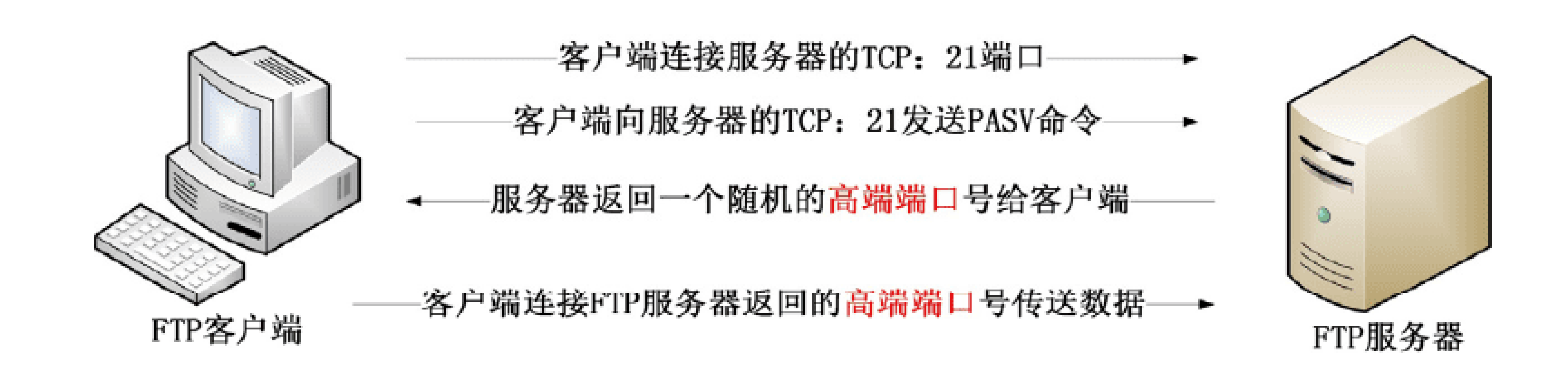


图 5-56　FTP 服务器的 PORT 模式

2. 被动模式（PASV）

PASV 模式在建立控制通道的时候和 PORT 模式类似，但建立连接后发送的不是 PORT 命令，而是 PASV 命令。FTP 服务器收到 PASV 命令后，随机打开一个高端端口（端口号大于 1024）并且通知客户端在这个端口上传送数据的请求，客户端连接 FTP 服务器此端口，然后 FTP 服务器将通过这个端口进行数据的传送，这个时候 FTP server 不再需要建立一个新的和客户端之间的连接，如图 5-57 所示。



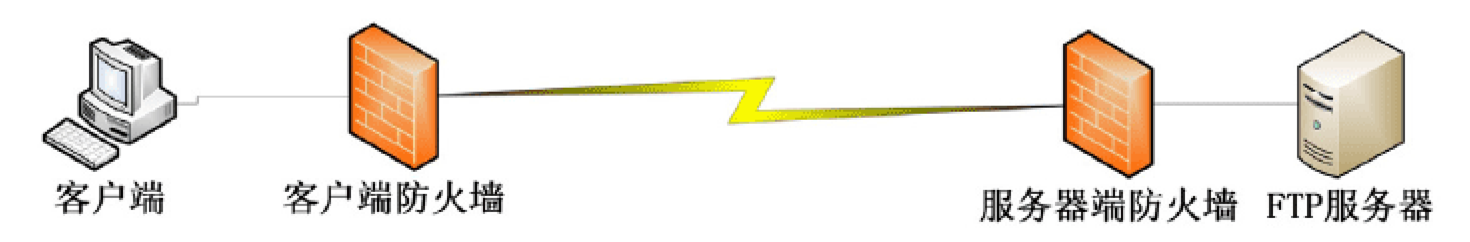
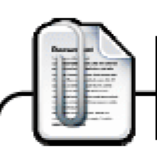


图 5-57　FTP 服务器的 PASV 模式

很多防火墙在设置的时候都是不允许接受外部发起的连接的，所以许多位于防火墙后或内网的 FTP 服务器不支持 PASV 模式，因为客户端无法穿过防火墙打开 FTP 服务器的高端端口；而许多内网的客户端不能用 PORT 模式登陆 FTP 服务器，因为从服务器的 TCP 20 端口无法和内部网络的客户端建立一个新的连接，造成无法工作。



说 明

关于如何配置防火墙后的 FTP 服务器、让 FTP 服务器可以为 Internet 的 FTP 客户端提供正常的服务，这些设置涉及到防火墙的内容，将在本书后面的章节介绍。

5.5.2　配置不隔离用户的 FTP 服务器

在“5.2 安装 Web 服务器”一节的时候，已经介绍了安装 Web 服务器的方法。本节将介绍 FTP 服务器的配置方法与步骤。

在 Windows Server 2008 中，FTP 服务器支持“用户隔离”功能。FTP 用户隔离为 Internet 服务提供商（ISP）和应用服务提供商（ASP）提供了解决方案，使他们可以为客户提供上载文件和 Web 内容的个人 FTP 目录。FTP 用户隔离通过将用户限制在自己的目录中，来防止用户查看或覆盖其他用户的 Web 内容。因为顶层目录就是 FTP 服务器的根目录，用户无法浏览目录树的上一层。在特定的站点内，用户能创建、修改或删除文件和文件夹。

FTP 用户隔离是站点属性，而不是服务器属性。可以为每个 FTP 站点启动或关闭该属性。

FTP 用户隔离支持下面三种隔离模式，其中每种模式启用不同级别的隔离和身份验证。

- 不隔离用户：此模式不启用 FTP 用户隔离。该模式的工作方式与以前版本的 IIS 类似。
- 隔离用户：此模式在用户可以访问与其用户名匹配的主目录前，根据本机或域账户对用户进行身份验证。
- 用 Active Directory 隔离用户：此模式根据相应的 Active Directory 容器验证用户凭据，而不是搜索整个 Active Directory，因为这样做需要大量的处理时间。

在安装 FTP 服务器的时候，默认情况下，安装的 FTP 服务器是以“不隔离用户”的方式启动

的。在 Windows Server 2008 中，配置 FTP 服务器的步骤如下。

01 从“开始→管理工具”中运行“Internet 信息服务（IIS）6.0 管理器”命令，打开“Internet 信息服务（IIS）6.0 管理器”，如图 5-58 所示，可以看到“FTP 站点”选项。

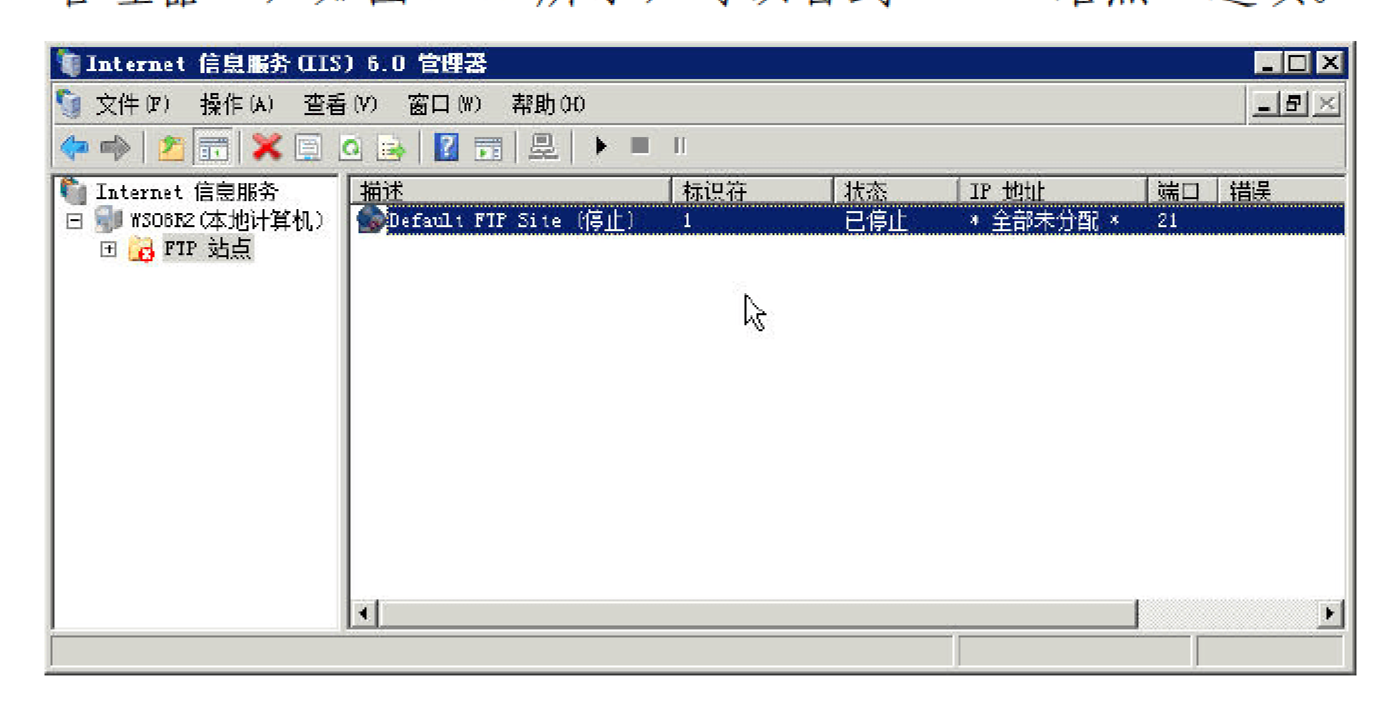
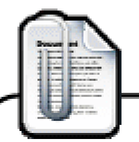


图 5-58 FTP 服务器



说 明

Windows Server 2008 中的 FTP 服务器，采用的是 IIS 6.0 版本，所以只能通过“Internet 信息服务（IIS）6.0 管理器”管理。而 Windows Server 2008 R2 中的 FTP 服务器，则是 IIS 7.5 版本，需要使用“Internet 信息服务（IIS）管理器”管理。

02 在默认情况下，FTP 服务器并没有启动，用户可以在右侧窗格中选中“Default FTP Site”，单击工具栏上的“▶”按钮，启动 FTP 服务器。当 FTP 服务器启动后，可以单击“■”按钮停止 FTP 服务器，或者单击“Ⅱ”按钮，暂时停止 FTP 服务器的运行。在第一次启动 FTP 服务器的时候，会弹出“不能更改此站点状态”的提示框，单击“是”按钮启动此服务和此站点即可，如图 5-59 所示。

03 用鼠标右击默认的 FTP 站点，在弹出的快捷菜单中，可以看到常用的 FTP 操作命令，例如“启动”、“停止”、“暂停”、“新建（FTP 站点、虚拟目录）”、“删除（删除 FTP 服务器）”、“重命名”、“属性”等命令，如图 5-60 所示。

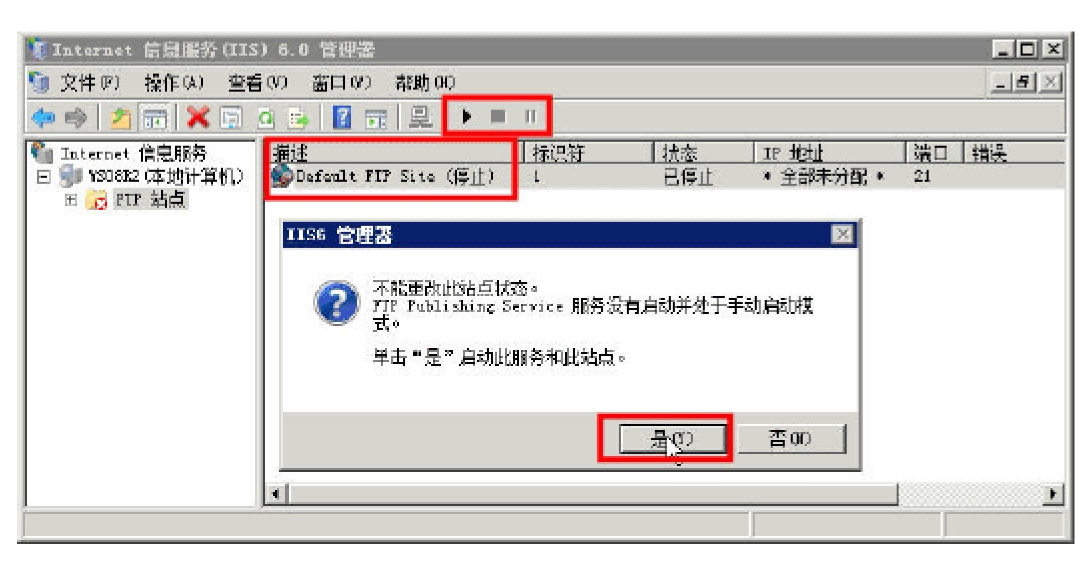


图 5-59 启动 FTP 服务器和站点

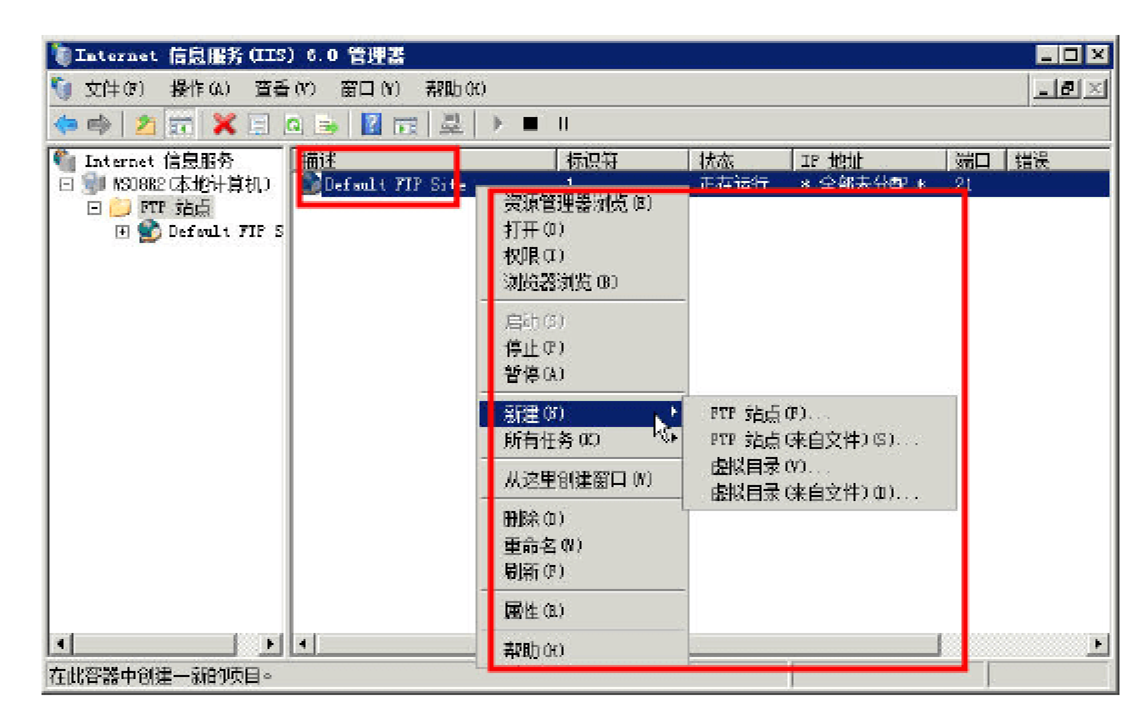


图 5-60 右键菜单命令

上述 FTP 的常用操作命令比较简单，大家可以通过命令的名称知道相应的功能，例如“停止”，是停止 FTP 服务器的命令。“新建→虚拟目录”，则是在当前 FTP 服务器中创建“虚拟目录”，这与

Web 服务器的虚拟目录的功能相同。

04 在图 5-60 中，选择“属性”选项，打开默认 FTP 站点的属性对话框，首先看到的是“FTP 站点”选项卡，在该选项卡中，可以修改 FTP 站点的描述信息、FTP 服务器绑定的 IP 地址、FTP 服务器的服务端口（TCP 默认为 21），以及 FTP 站点的连接设置、连接超时等，如图 5-61 所示。管理员可以根据需要或自己的爱好，设置或修改该 FTP 站点的信息。单击“当前会话”按钮，会显示当前连接到 FTP 服务器的客户端的信息。

05 在“安全账户”选项卡中，设置“匿名连接”的消息，默认情况下是“允许匿名连接”，如图 5-62 所示。

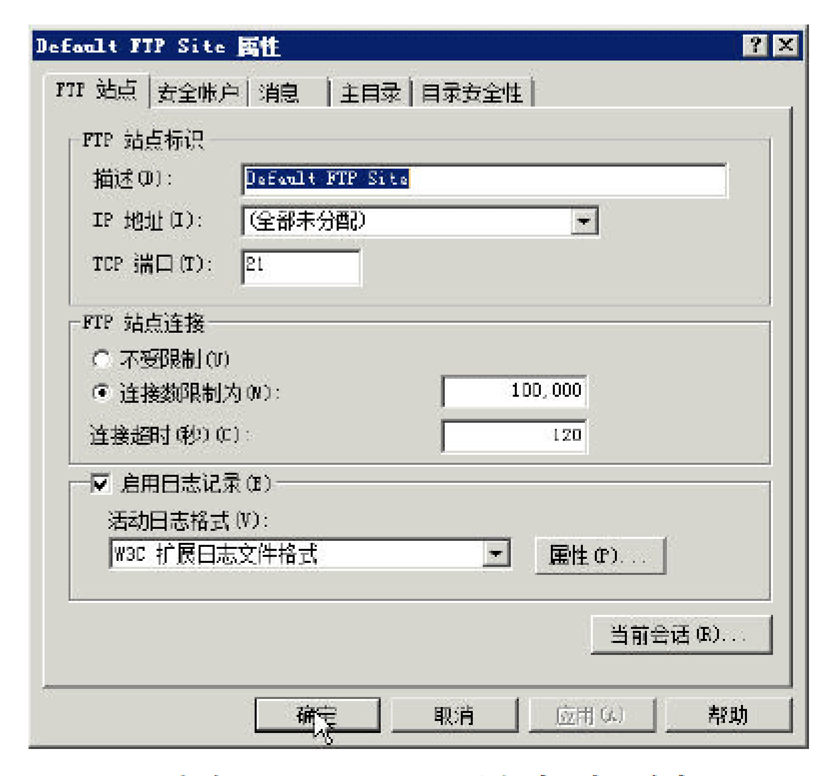


图 5-61　FTIP 站点选项卡

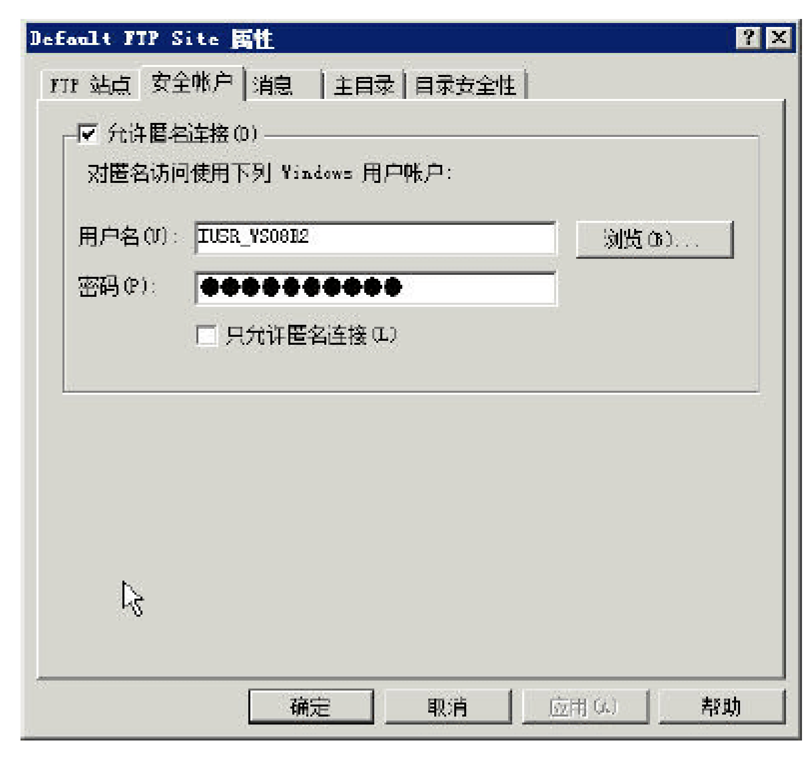


图 5-62　安全账户

说 明

不要更改匿名连接的用户名，通常情况下，IIS 中的匿名账户是 IUSR+（下划线）+（服务器计算机名称），如果在安装 Web 服务器之后，更改了计算机名称，Internet 匿名账户将会使用原来的计算机名称。如果选中“只允许匿名连接”，则只能是匿名连接，不允许使用其他账户登录。

06 在“消息”选项卡中可以创建在用户连接到 FTP 站点时显示的横幅、欢迎和退出消息。

在“横幅”文本框中，可以输入标题消息。在客户端连接到 FTP 服务器之前，该服务器将显示此消息。默认情况下消息为空。在“欢迎”文本框中输入欢迎消息。在客户端连接到 FTP 服务器时，该服务器将显示此消息。默认情况下消息为空。在“退出”文本框中输入退出消息。在客户端注销 FTP 服务器时，该服务器将显示此消息。默认情况下消息为空。

在“最大连接数”文本框中输入最大连接数消息。在客户端试图连接到 FTP 服务器但由于 FTP 服务已达到允许的最大客户端连接数而失败时，该服务器显示此消息。默认情况下消息为空。

管理员可以根据需要，对此进行设置，如图 5-63 所示。

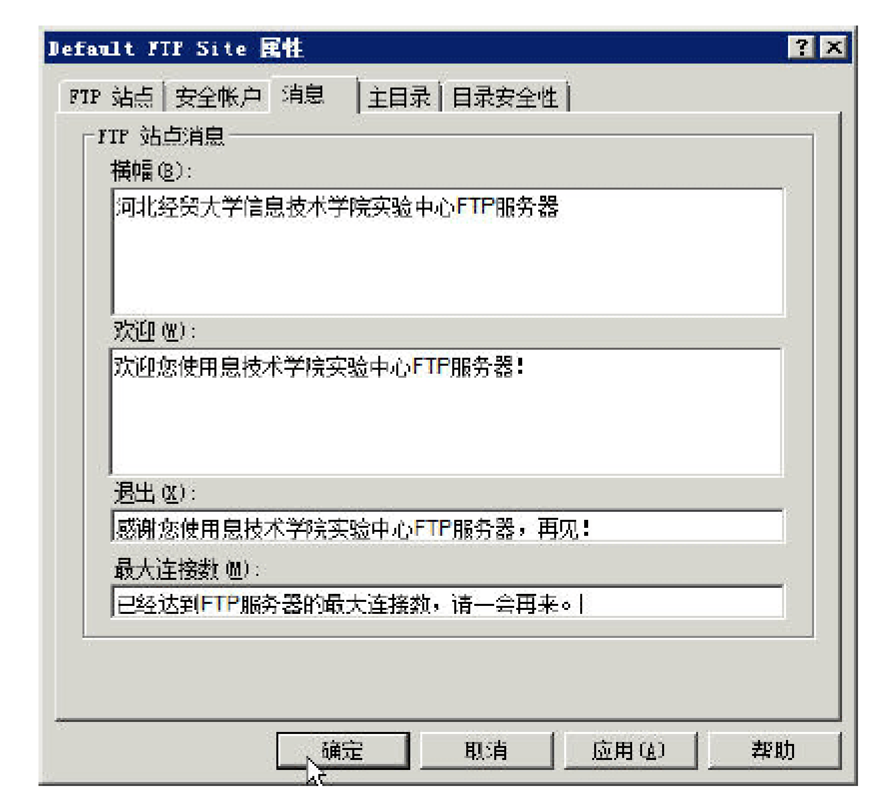


图 5-63　消息

07 在“主目录”选项卡中可以更改 FTP 站点的主目录或修改其属性。主目录是 FTP 站点中用于已发布文

件的中心位置。在安装 FTP 服务时，系统已创建默认主目录，并将其存储在 %systemdrive%\inetpub\ftproot 中。

用户可以将主目录的位置更改为下列任意一个：

选中“此计算机上的目录”时，可以允许用户访问此计算机上的指定目录，以便查看或更新 FTP 内容。用户可以执行任何 Windows 安全方法来控制对内容的访问。在“本地路径”文本框中，输入目录或目标 URL 的路径，语法必须与当前所选的路径类型相匹配。对于本地目录，须使用完整路径，例如 C:\inetpub\ftproot，如图 5-64 所示。对于网络共享，须使用通用命名约定（UNC）服务器和共享名，例如 \\Webserver\htmlfiles。

如果选中“另一台计算机上的目录”时，可以允许用户查看或更新与该计算机有活动连接的其他计算机上的 FTP 内容。如果用户具有远程计算机上的管理凭据，那么可以通过执行任何 Windows 安全方法来控制对其内容的访问。用户可以在“网络共享”框中输入服务器名和目录名，如图 5-65 所示。单击“连接为”按钮可以输入或更改网络用户名和密码信息。

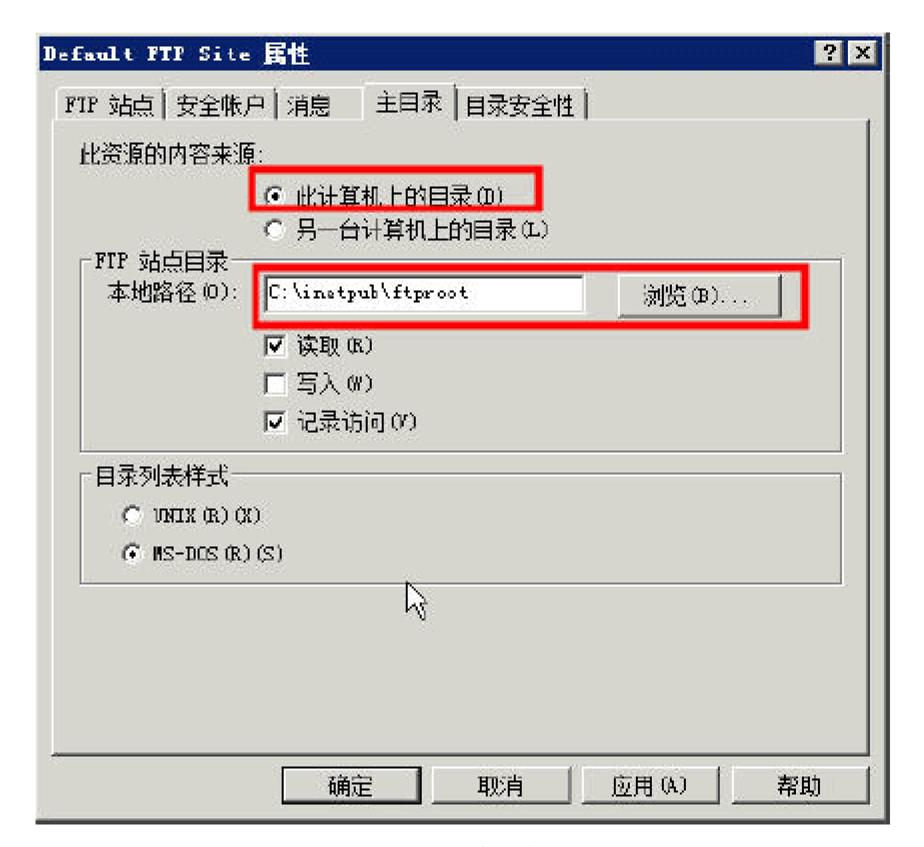


图 5-64　此计算机上的目录

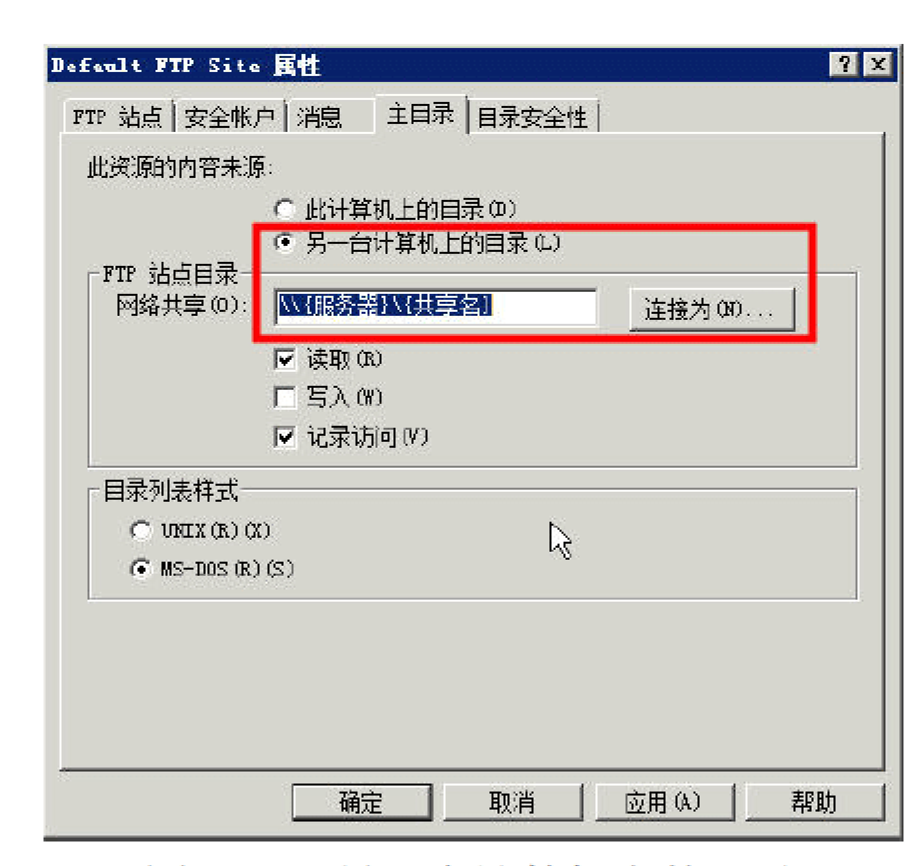


图 5-65　另一台计算机上的目录

在选中“读取”复选框时，该选项可以允许用户读取或下载存储在主目录或虚拟目录中的文件。在选中“写入”复选框时，该选项可以允许用户向服务器中已启用的目录上载文件。应该仅对要接收用户文件的目录启用写入权限。在选中“记录访问”复选框时，此选项可以将对该目录的访问记录到日志文件中。只有为该 FTP 站点启用了日志记录时才记录访问。默认情况下启用日志记录。

在“目录列表样式”选项组中，设置允许用户在 MS-DOS 和 UNIX 样式目录列表之间进行选择。在选择“UNIX”时，可以在文件的日期与 FTP 服务器的年份不同时使用四位数字格式显示年份。如果文件日期与 FTP 服务器的年份相同，则不返回年份。在选择“MS-DOS”时，可以在默认情况下用两位数字格式显示日期中的年份。

08 在“目录安全性”选项卡中，可允许或阻止单个计算机或计算机组访问 FTP 站点。这与在 Web 服务器中，允许或拒绝指定的 IP 地址访问 Web 服务器是相同的功能，如图 5-66 所示。

单击“授权访问”单选按钮，可将访问权限授予所有计算机，这也是默认的设置。如果要添加拒绝访问的计算机、计算机组或域，须单击“添加”按钮，然后在“拒绝访问”对话框中输入所需

的信息。被拒绝访问的计算机将出现在“下列除外”列表框中。



图 5-66　目录安全性

如果单击“拒绝访问”单选按钮，可以拒绝所有计算机的访问权限。要添加允许访问的计算机、计算机组或域，须单击“添加”按钮，然后在“授权访问”对话框中输入所需的信息。授权访问的计算机出现在“下列除外”列表框中。

用户可以根据需求配置 FTP 服务器，设置完成之后，单击“确定”按钮。

5.5.3　配置隔离用户的 FTP 服务器

创建隔离用户的 FTP 服务器，在创建每个用户的 FTP 站点目录时，请遵循以下惯例：

- 如果允许匿名访问，则在 FTP 站点主目录下创建 LocalUser 和 LocalUser\Public 子目录。
- 如果本地计算机用户使用他们各自的账户用户名登录（而不是作为匿名用户），则在 FTP 站点主目录下为每个允许连接到该 FTP 站点的用户创建 LocalUser 子目录以及一个单独的 LocalUser\UserName 目录。
- 如果不同域的用户使用显式 Domain\UserName 凭据登录，则在该 FTP 站点根目录下为每个域都创建一个子目录（使用域名）。在每个域目录下，为每个用户创建一个目录。例如，要支持用户 Contoso\user1 访问，请创建 Contoso 和 Contoso\user1 目录。

下面，我们通过具体的实例，介绍创建隔离用户 FTP 服务器的方法与步骤，实现如下的功能：

创建 FTP 服务器，在“计算机管理→系统工具→本地用户和组”中创建两个用户 ws01、ws02，当 FTP 客户端以用户 ws01 登录时，可以浏览、读写 E:\web1 文件夹的权限；当 FTP 客户端以用户 ws02 登录时，具有读写 E:\web2 文件夹的权限。

01 在“本地用户和组→用户”中，创建两个账户，分别为 ws01、ws02，如图 5-67 所示。

02 在 E 盘根目录创建 ftp-root 文件夹，在 ftp-root 中创建 LocalUser 文件夹，在 LocalUser 中创建 Public、ws01、ws02 文件夹，分别在 ws01、ws02 中创建同名文本文件，例如在 ws02 中创建名为 ws02.txt 的文件，如图 5-68 所示。这样，当用户测试的时候，将很容易分辨出当前所在的

目录。

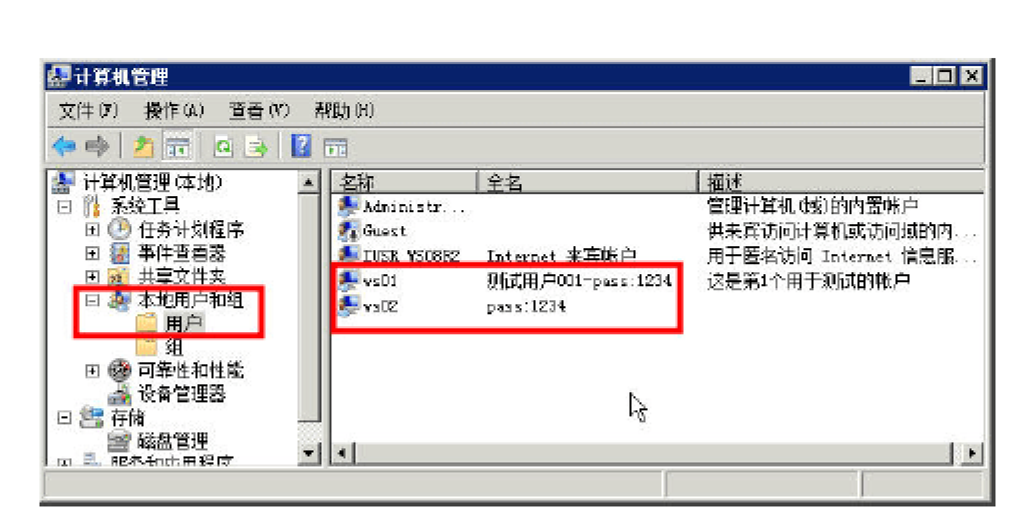




图 5-67　创建两个用户

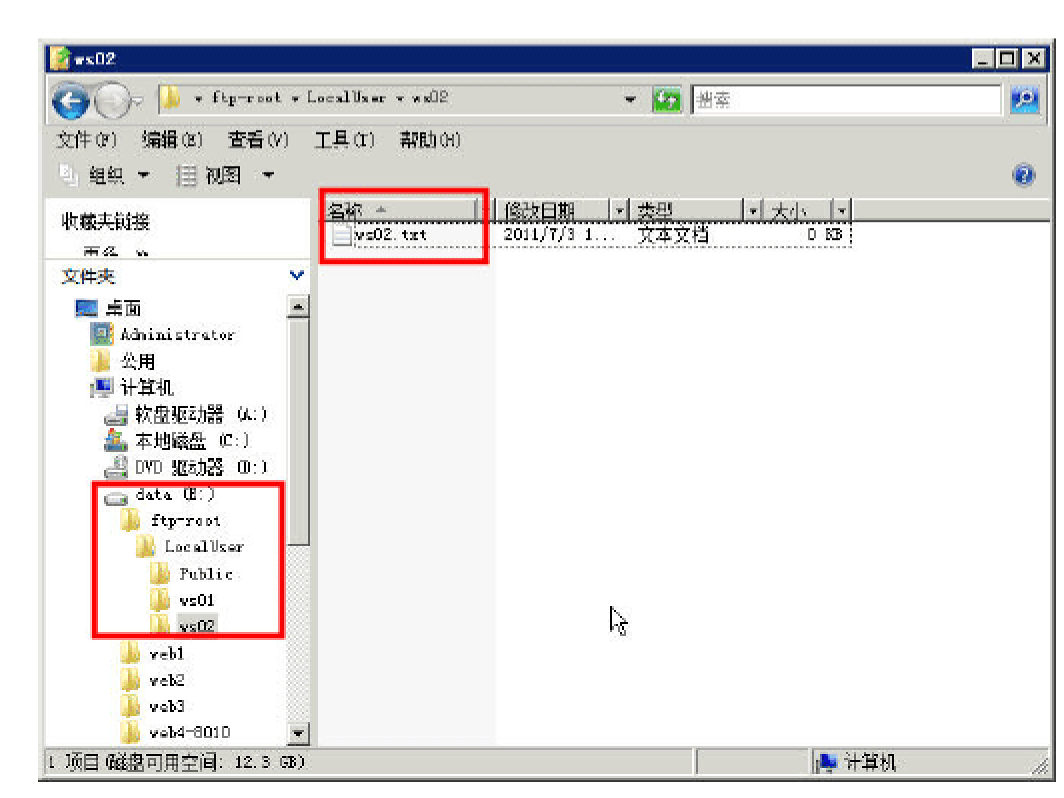


图 5-68　创建文件夹并创建同名文本文件

03 在 E:\web1、E:\web2 文件夹创建同名文本文件，然后修改 web1 的 NTFS 权限，只允许 Administrator、ws01 具有“完全控制”权限，允许 Everyone 有“读取权限”，如图 5-69 所示。

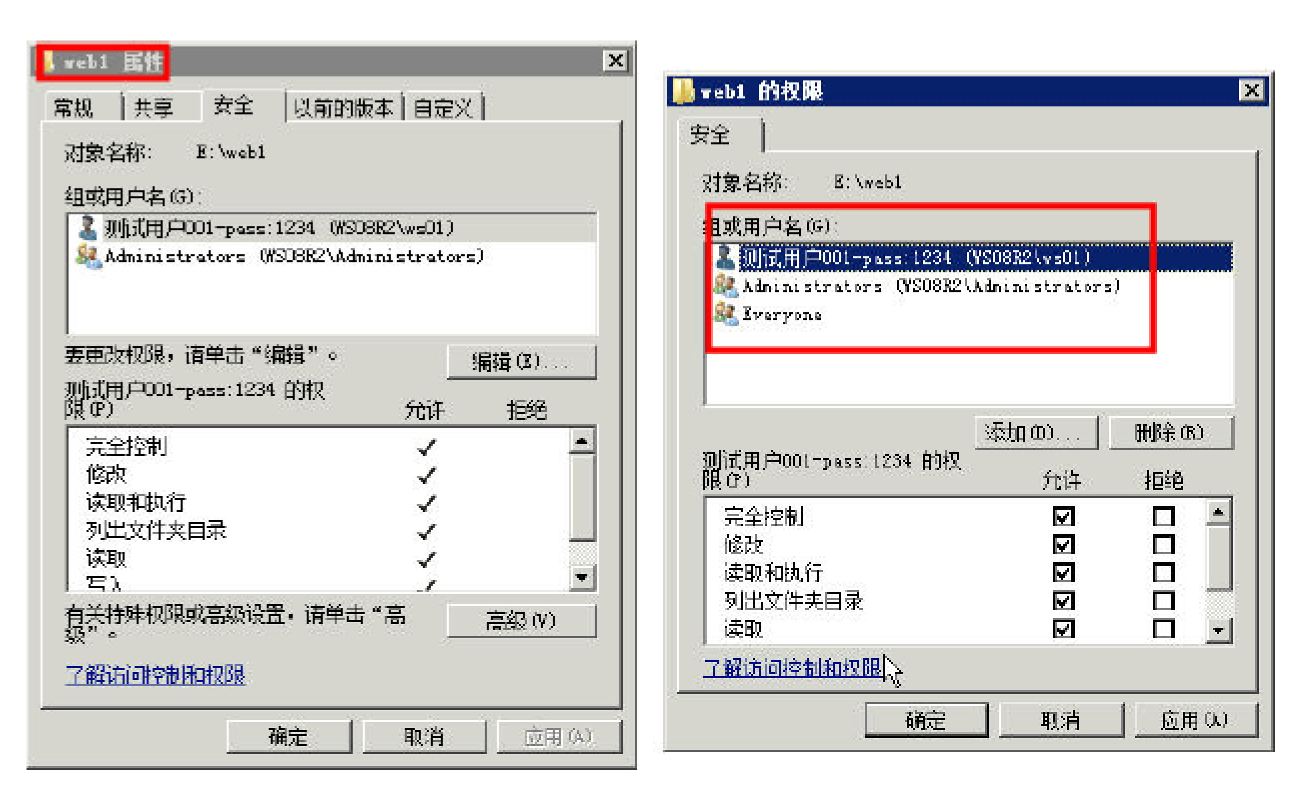


图 5-69　修改 E:\web1 的 NTFS 权限

同样，对于 web2，也要修改它的 NTFS 权限，只允许 Administrator、ws02 具有“完全控制”权限，允许 Everyone 有“读取权限”。

04 然后返回到“Internet 信息服务（IIS）6.0 管理器”，删除“Default FTP Site”站点，然后用鼠标右击“FTP 站点”，在弹出的快捷菜单中选择“新建→FTP 站点”选项，如图 5-70 所示。

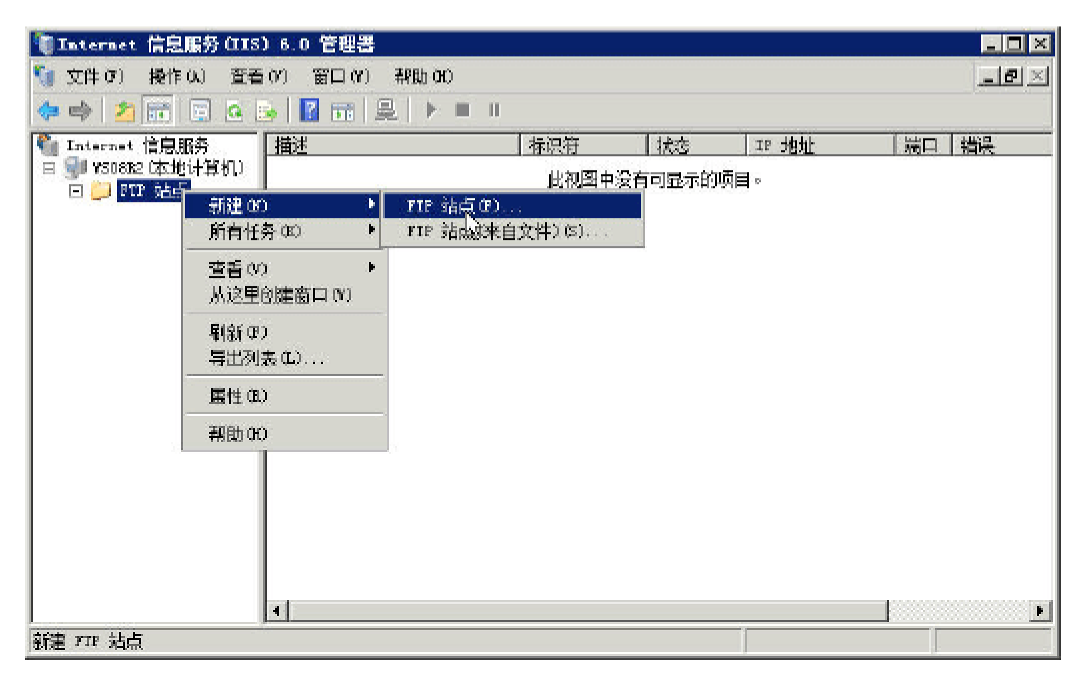


图 5-70　新建 FTP 站点

05 在“FTP 站点描述”对话框中，输入当前新建 FTP 站点的描述信息，例如 FTP，如图 5-71 所示。

06 在“IP 地址和端口设置”对话框，保持默认值，如图 5-72 所示。也可以根据需要，选择 FTP 服务器绑定的 IP 地址及服务端口。



图 5-71　FTP 站点描述

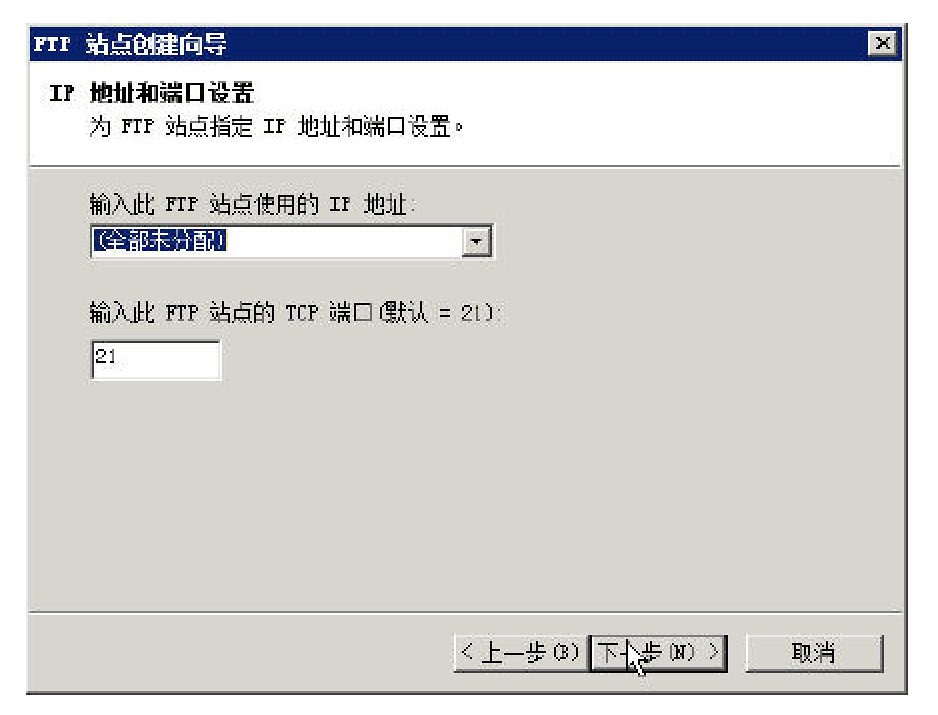


图 5-72　IP 地址和端口设置

07 在“FTP 用户隔离”对话框中，单击“隔离用户”单选按钮，如图 5-73 所示。

08 在“FTP 站点主目录”对话框中，选择新建 FTP 服务器的根目录，在本例中，该目录为 E:\ftp-root，如图 5-74 所示。

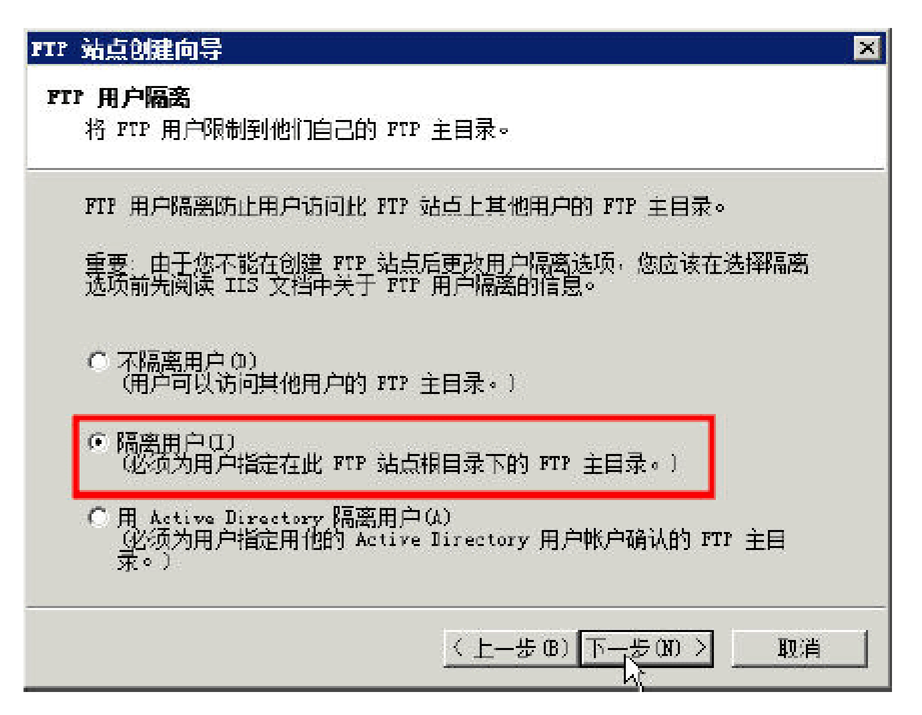


图 5-73　隔离用户

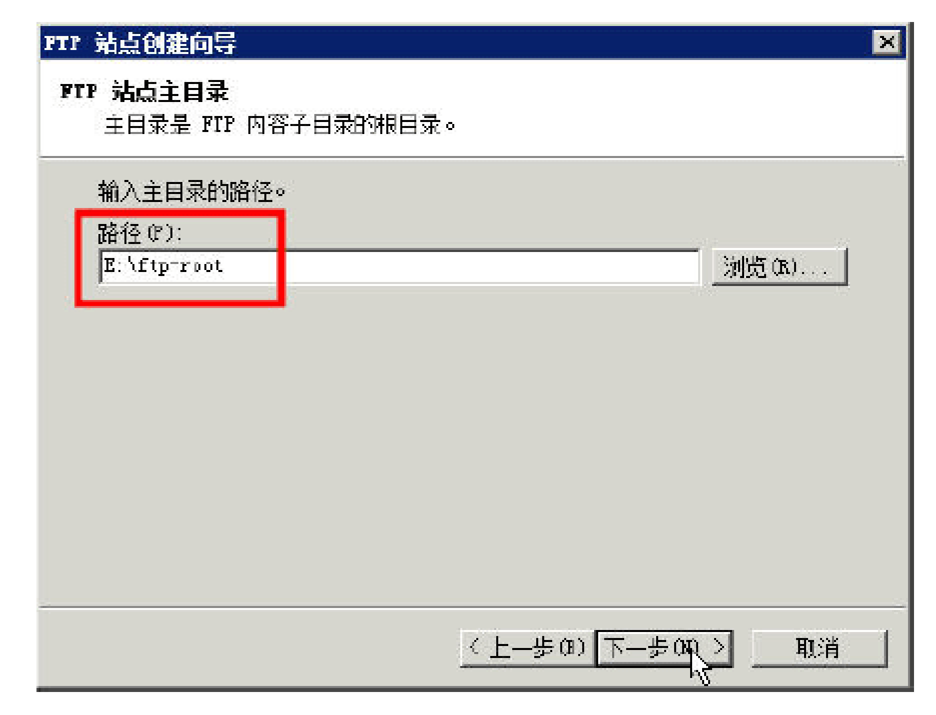


图 5-74　指定 FTP 站点主目录

09 在“FTP 站点访问权限”对话框中，选中此 FTP 站点的访问权限，在此选中“读取”和“写入”复选框，如图 5-75 所示。

10 在“已成功完成 FTP 站点创建向导”对话框中，单击“完成”按钮，如图 5-76 所示。

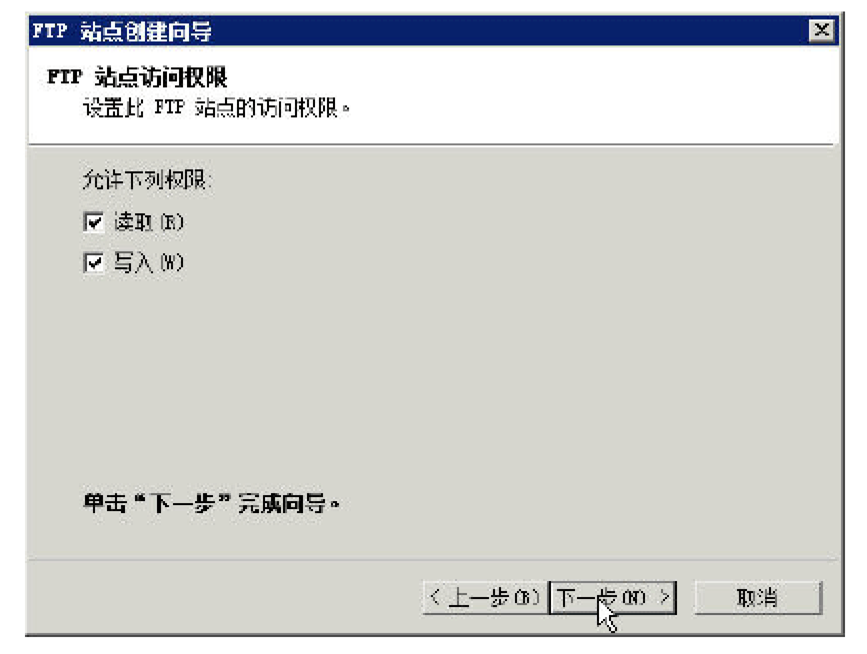


图 5-75　FTP 站点访问权限

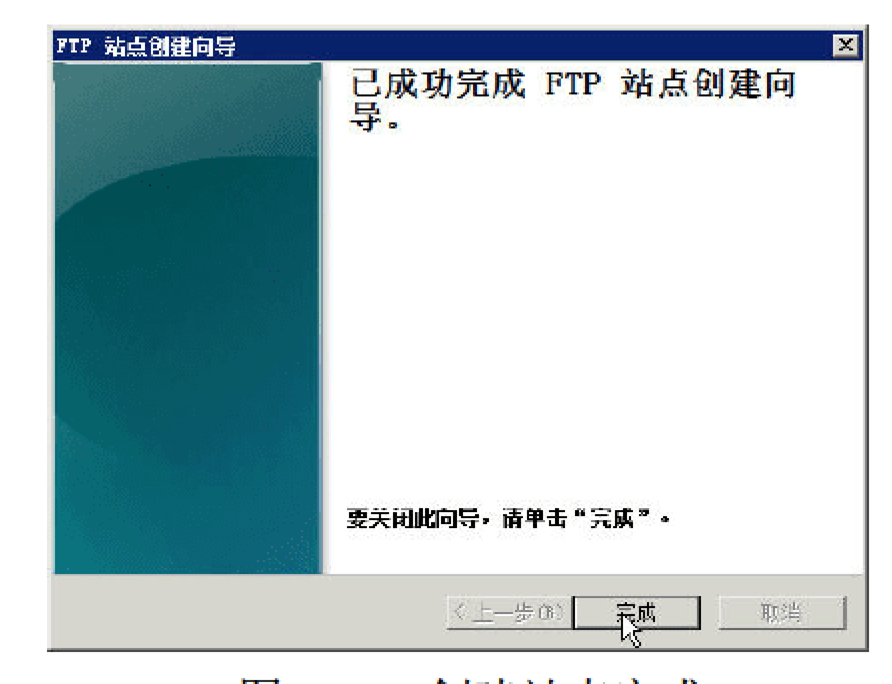


图 5-76　创建站点完成

11 在创建 FTP 站点之后，还要创建两个虚拟目录，指向 E:\web1 与 E:\web2。用鼠标右击“FTP”，在弹出的快捷菜单中选择“新建→虚拟目录”命令，如图 5-77 所示。

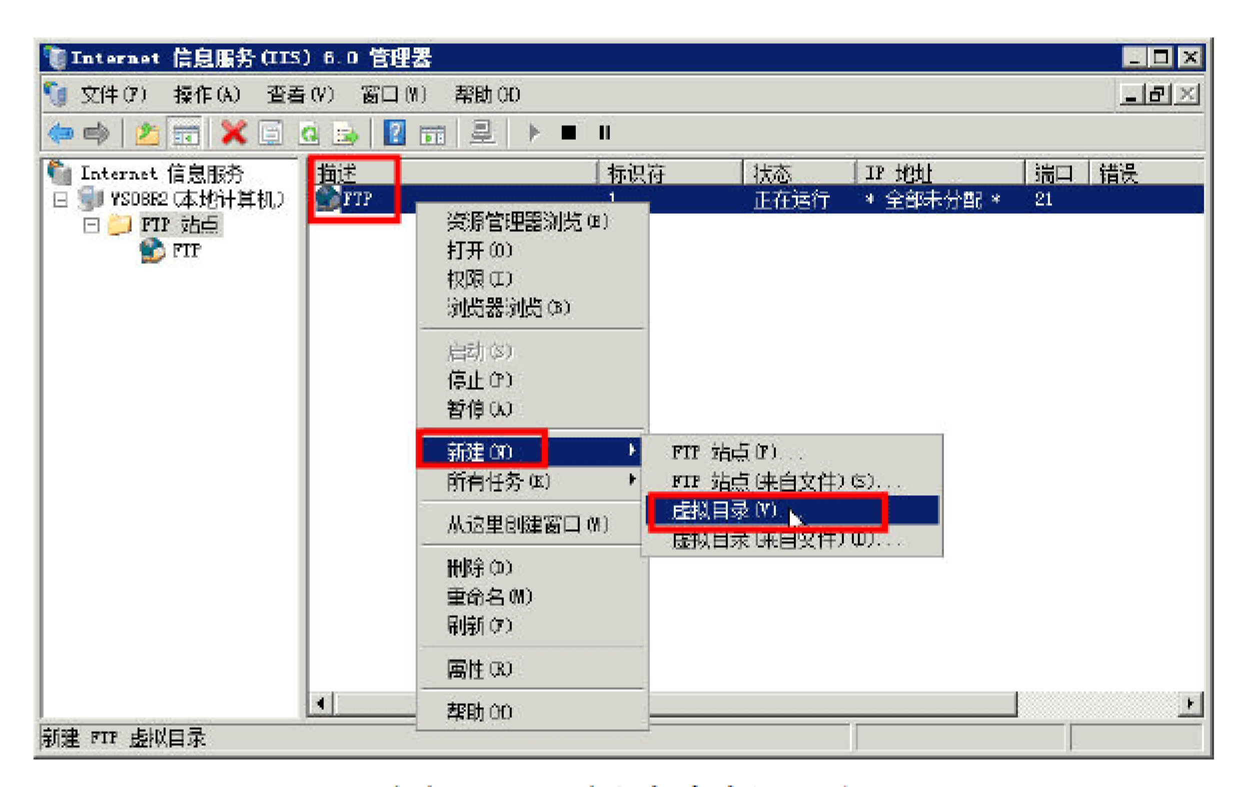


图 5-77　新建虚拟目录

12 在“虚拟目录别名”对话框中，设置别名为 web1（如图 5-78 所示），该别名将指向 E:\web1 文件夹，如图 5-79 所示。

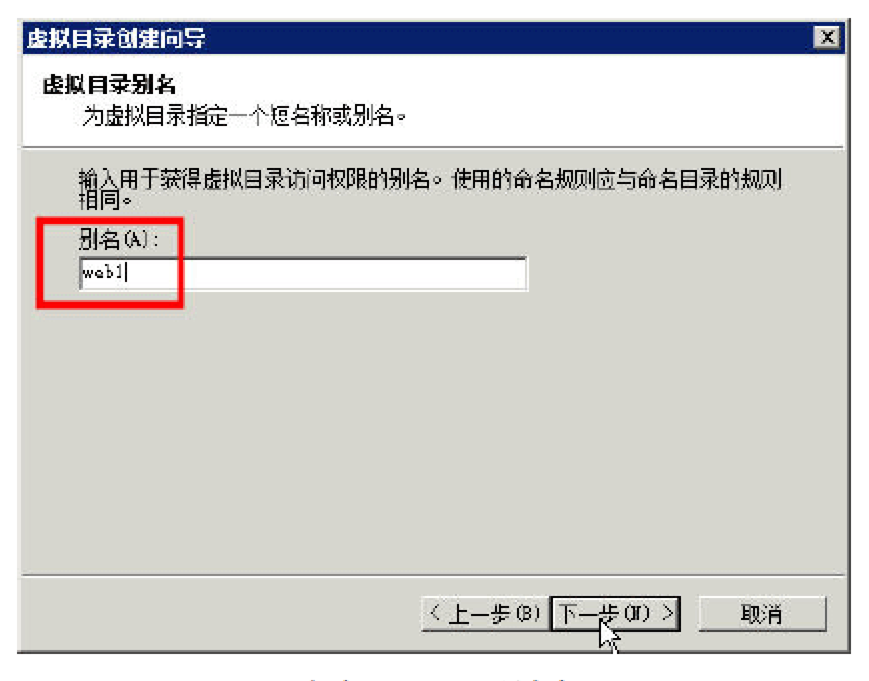


图 5-78　别名

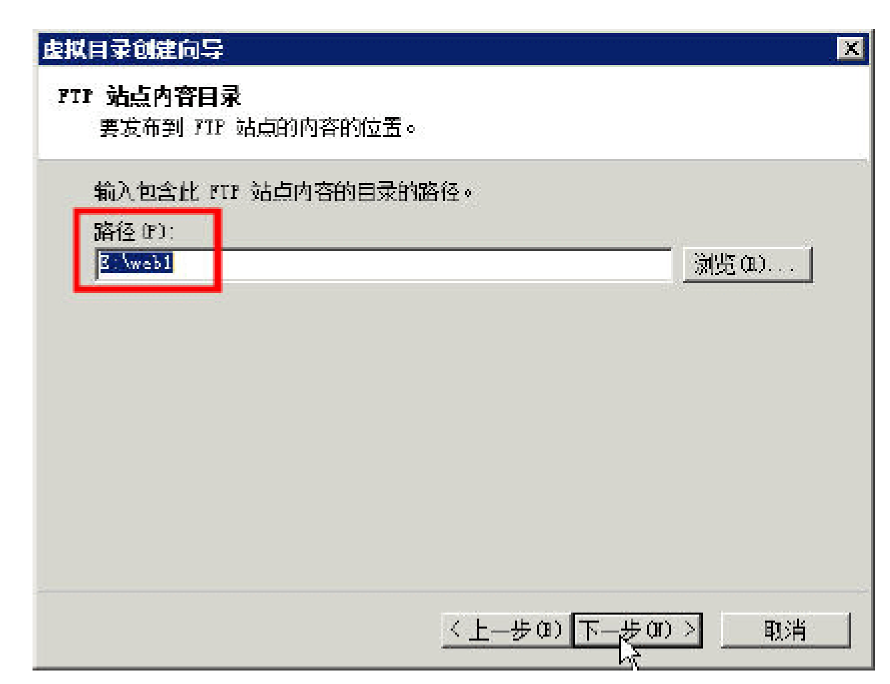


图 5-79　指定站点内容目录

13 在“虚拟目录访问权限”对话框中，选中“读取”和“写入”权限，如图 5-80 所示。

14 在“已成功完成虚拟目录创建向导”对话框中，单击“完成”按钮，完成 web1 虚拟目录的创建，如图 5-81 所示。

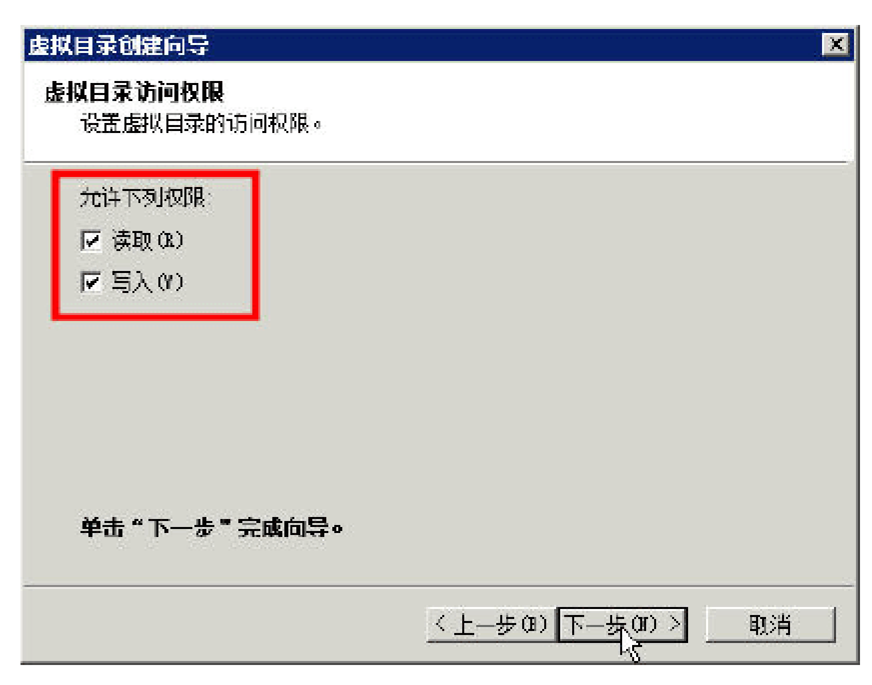


图 5-80　虚拟目录访问权限

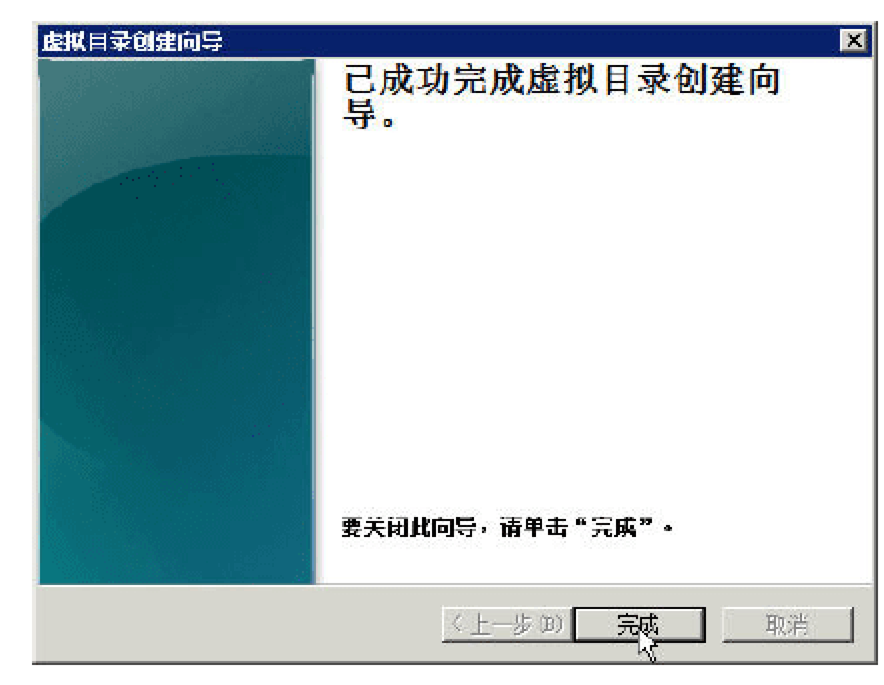


图 5-81　创建虚拟目录完成

15 然后参照步骤 11～14，为 E:\web2 创建名为 web2 的虚拟目录。

5.5.4 测试隔离 FTP 服务器

在创建好隔离用户的 FTP 服务器、设置好虚拟目录、设置好各目录的权限之后，我们将根据 5.5.3 小节的要求，测试隔离用户 FTP 服务器，测试步骤如下。

01 在 IE 浏览器中，输入 FTP 服务器的地址“ftp://192.168.1.10”，按回车键，然后在“页面”菜单中选择“在 Windows 浏览器中打开 FTP”选项，如图 5-82 所示。

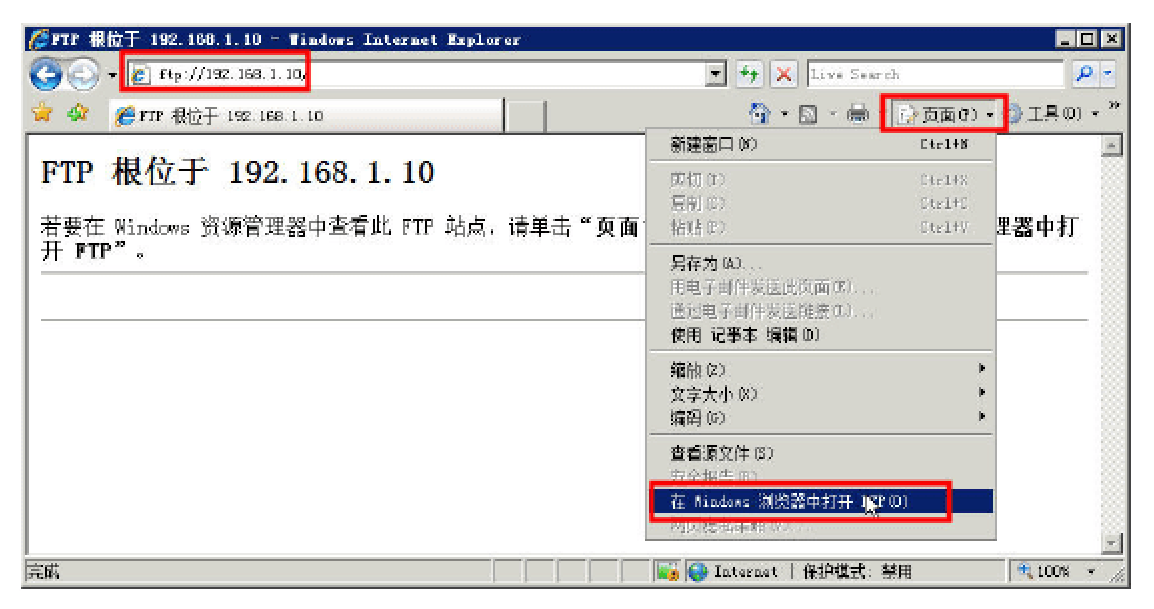


图 5-82 在 Windows 浏览器中打开 FTP

02 使用 Windows 浏览器打开 FTP 之后，在右侧的窗格中单击鼠标右键，在弹出的快捷菜单中选择“登录”按钮，如图 5-83 所示。

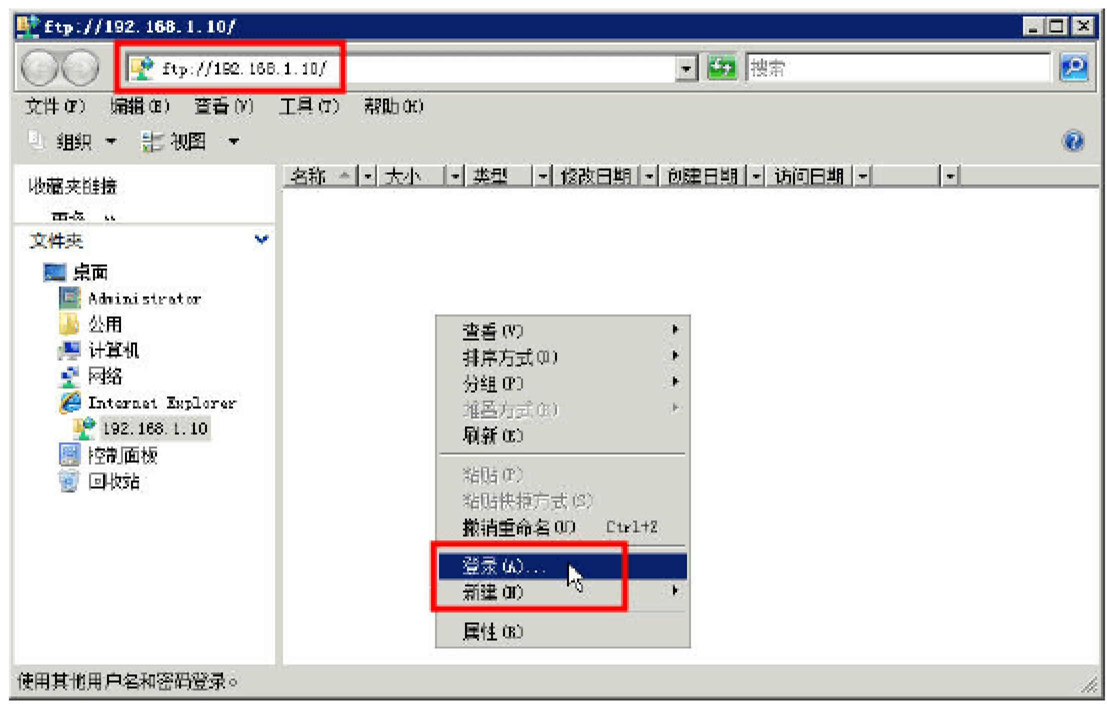


图 5-83 登录

03 在弹出的“登录身份”对话框中，使用用户名 ws01 及其密码登录（如图 5-84 所示），登录之后，进入 ws01 的主目录，如图 5-85 所示。

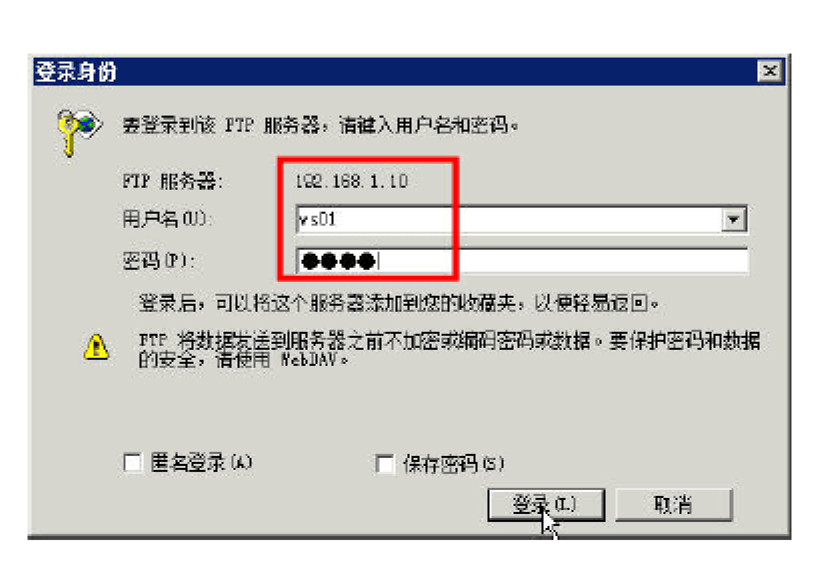


图 5-84 用 ws01 登录

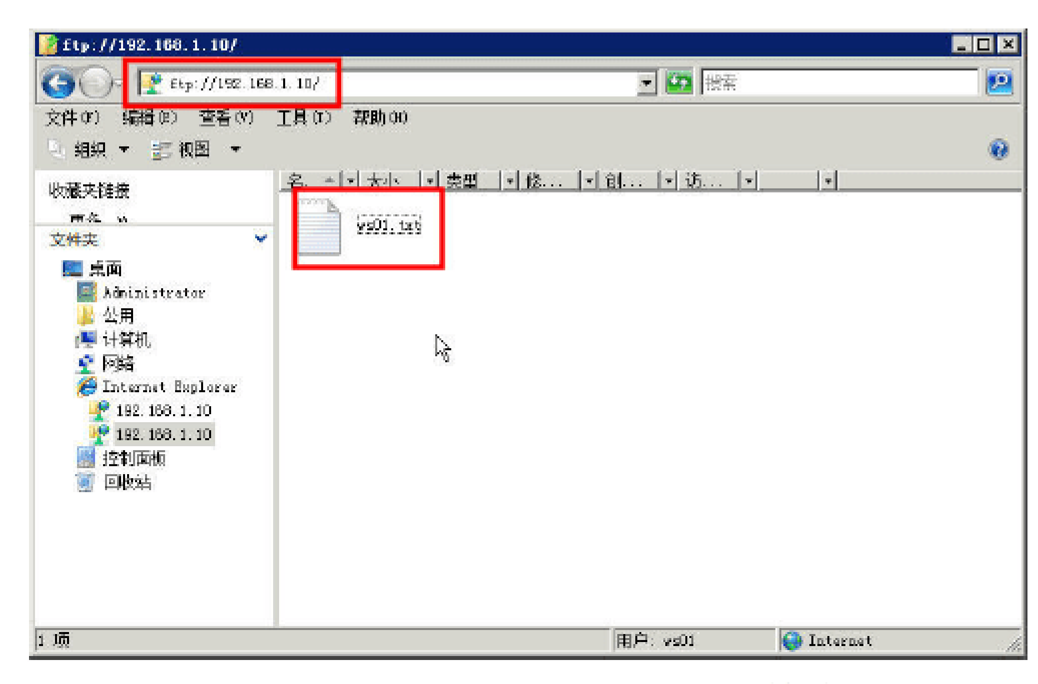


图 5-85 进入 ws01 文件夹

04 然后，在 ftp 地址栏后面添加 web1 的虚拟目录，并按回车键，进入 web1 所在的文件夹，如图 5-86 所示。登录之后，用户可以在此文件夹中，删除或新建文件，也可以从本地复制文件、文件夹上传（粘贴）到该目录。

05 由于当前登录的用户 ws01 对服务器所在目录 E:\web1 具有“完全控制”权限，所以，如果是“新建→文件夹”操作，是可以创建成功的，如图 5-87 所示。

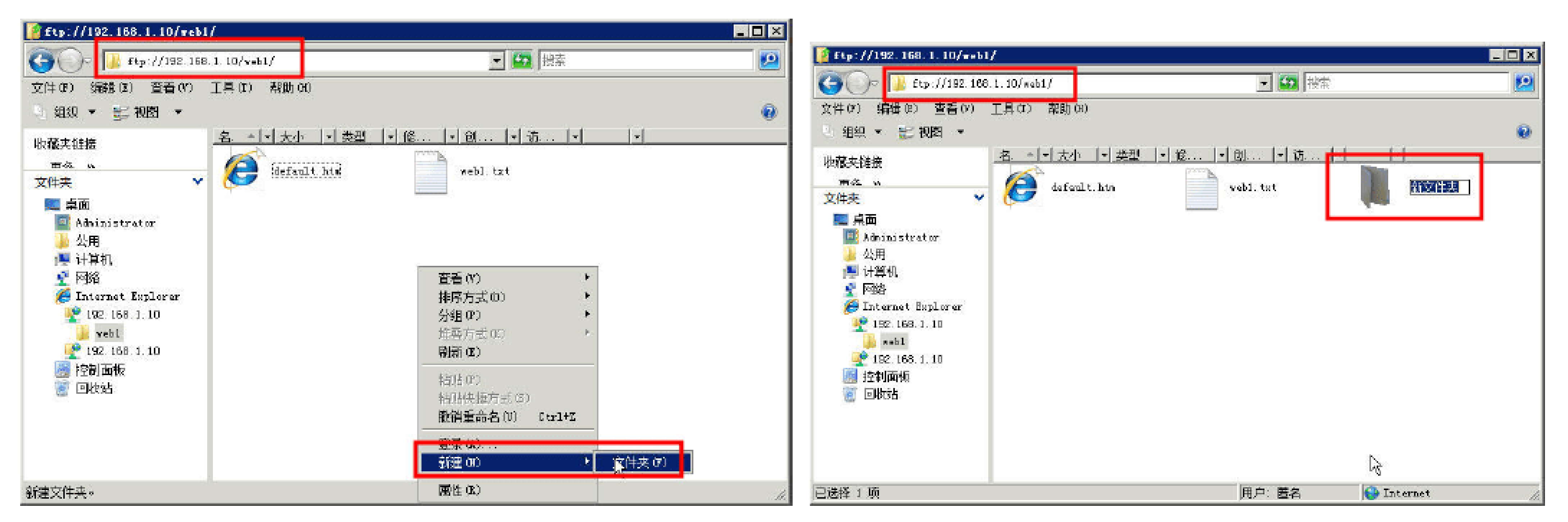


图 5-86　进入 web1 虚拟目录（对应服务器 E:\web1 文件夹）　　图 5-87　创建文件夹成功

06 如果此时登录 web2 虚拟目录，在尝试新建文件夹时，会出现“550 新文件夹：Access is denied”的错误，如图 5-88 所示。

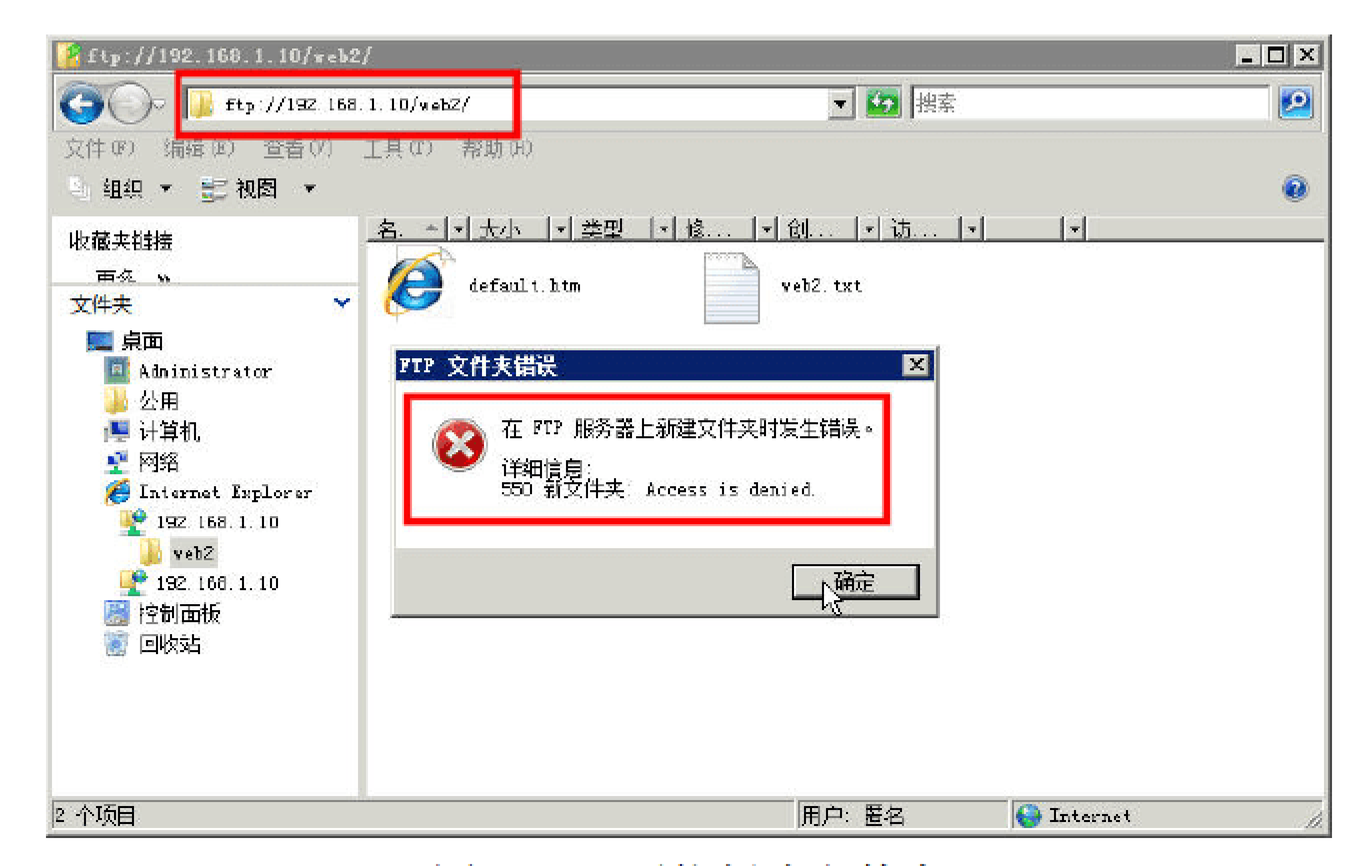


图 5-88　不能创建文件夹

然后，用户可以使用 ws02 登录，查看 ws02 读写 web1、web2 虚拟目录的情况，这些不再一一介绍。

5.6　应用案例：使用 Windows Server 2008 R2 打造双线 FTP 服务器

前文介绍过，在所有的网络服务中，FTP 服务器的发布是比较复杂的，这是由 FTP 的工作原理造成的。由于很多防火墙在设置的时候都是不允许接受外部发起的连接的，所以许多位于防火墙后

或内网的 FTP 服务器不支持 PASV 模式，因为客户端无法穿过防火墙打开 FTP 服务器的高端端口；而许多内网的客户端不能用 PORT 模式登陆 FTP 服务器，因为从服务器的 TCP 20 端口无法和内部网络的客户端建立一个新的连接，造成无法工作。

许多情况下，最终用户没有机会配置所属网络的防火墙。所以，为了解决这个问题，在发布 FTP 服务器时，通常是让 FTP 服务器工作在 PASV 模式，并且指定 PASV 对外服务的地址以及 PASV 服务的端口，让防火墙发布指定的端口。

以前笔者一直使用 serv-u 做 FTP 服务器，因为笔者的网络中有不止一台 FTP 服务器要发布到 Internet 供用户使用。在 Windows Server 2008 及其以前的版本中，虽然 Windows 操作系统自带的 FTP 服务器非常安全，但由于其配置较少，并且不能指定 PASV 端口对外地址、修改 PASV 端口范围较复杂等因素，所以一直使用 serv-u 等 FTP 服务器软件。但是，随着 64 位 Windows 操作系统的普及与发展，现在在网络中配置 FTP 又被提上了日程。支持 64 位 Windows Server 操作系统的 FTP 并不是很多，并且这些 FTP 服务器越来越庞大、复杂，偶尔会有漏洞出现。而对于我们大部分用户来说，需要 FTP 服务器的功能有限，能发布到 Internet、上传、下载，并能分用户管理就可以了。目前，Windows Server 2008 R2 升级了 IIS 中集成的 FTP 服务器，除了具有原来的功能外，还增加了指定 PASV 地址与端口的功能，这足以满足用户的需求。在接下来的文章中，我们通过一个案例进行介绍。

5.6.1　FTP 服务器实验案例

本案例中，使用 Forefront TMG 2010 进行实验。在图 5-89 中，由 Forefront TMG 2010 保护的内网中，有两台 FTP 服务器，这两台 FTP 服务器除了供内网使用外，还发布到 Internet，供 Internet 用户使用。并且，该网络外接有电信与联通线路，可以让用户根据自己的网络选择是使用电信还是联通线路连接到 FTP 服务器。

要实现图 5-89 所描述的网络功能，我们可以采用多种方法，在此先采用一个以前在 serv-u 中采用的办法：用不同的端口发布 FTP 服务器，我们通过表 5-2 对此做出规则。

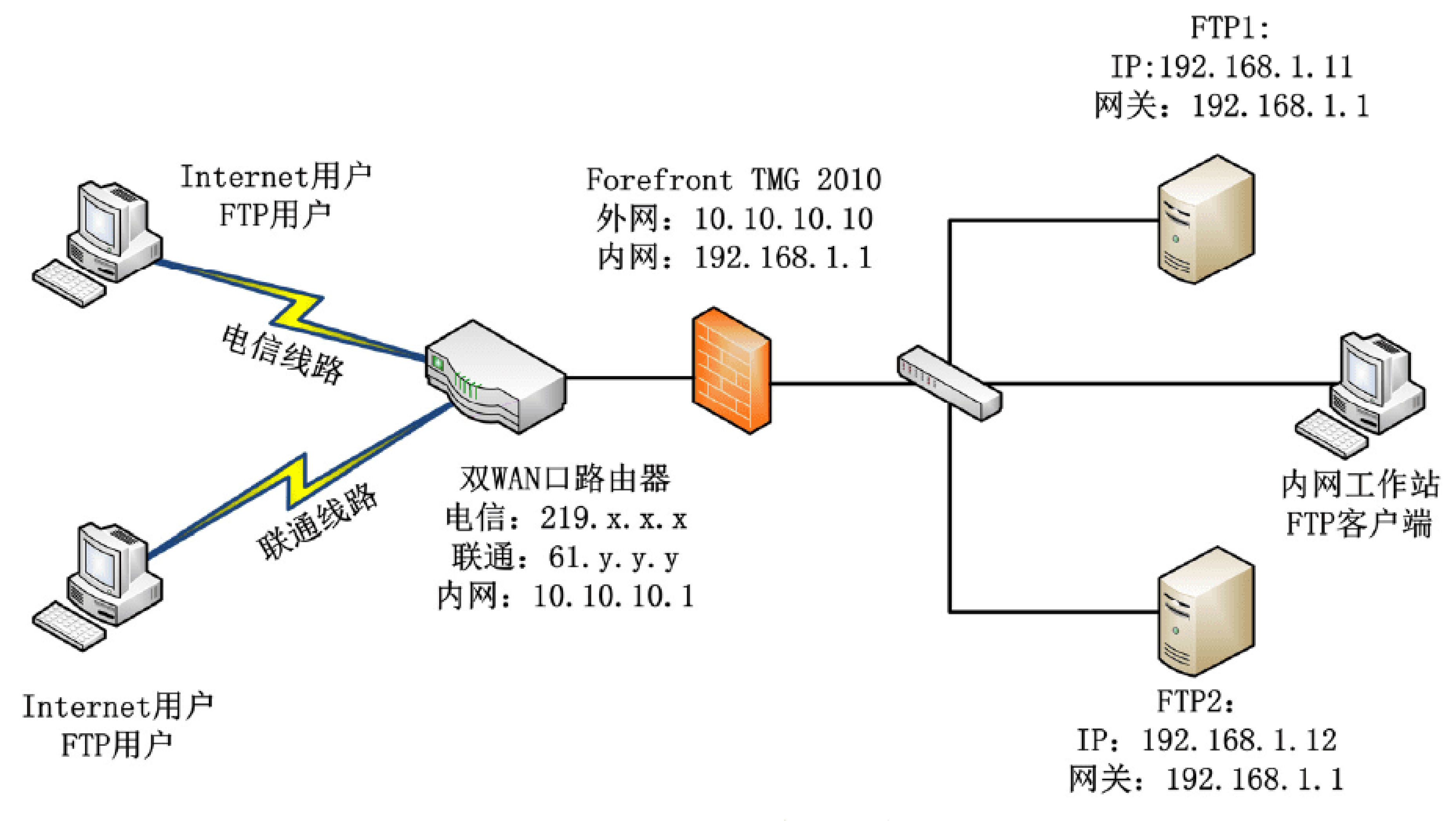


图 5-89　FTP 实验拓扑

表 5-2 双线 FTP 服务器相关信息

服务器	电信服务端口	联通服务端口	PASV 端口	内网服务端口
FTP1	2010	2011	2012	21
FTP2	2020	2021	2022	21

在按照表 5-2 规划完成后，Internet 的用户如果使用电信线路，则通过 ftp://219.x.x.x:2010 访问 FTP1，通过 ftp://219.x.x.x:2020 访问 FTP2；如果使用联通线路，则通过 ftp://61.y.y.y:2011 访问 FTP1，通过 ftp://61.y.y.y:2021 访问 FTP2；而内网用户，则直接通过 ftp://192.168.1.11 访问 FTP1，再通过 ftp://192.168.1.12 访问 FTP2。做好规划之后，实现起来就比较简单了，这里不再讨论。

5.6.2 双 WAN 口路由器设置

在双 WAN 口路由器中，映射 TCP 的 2010、2011、2012、2020、2021、2022 到 Forefront TMG 2010 的“外网地址”10.10.10.10，如图 5-90 所示。

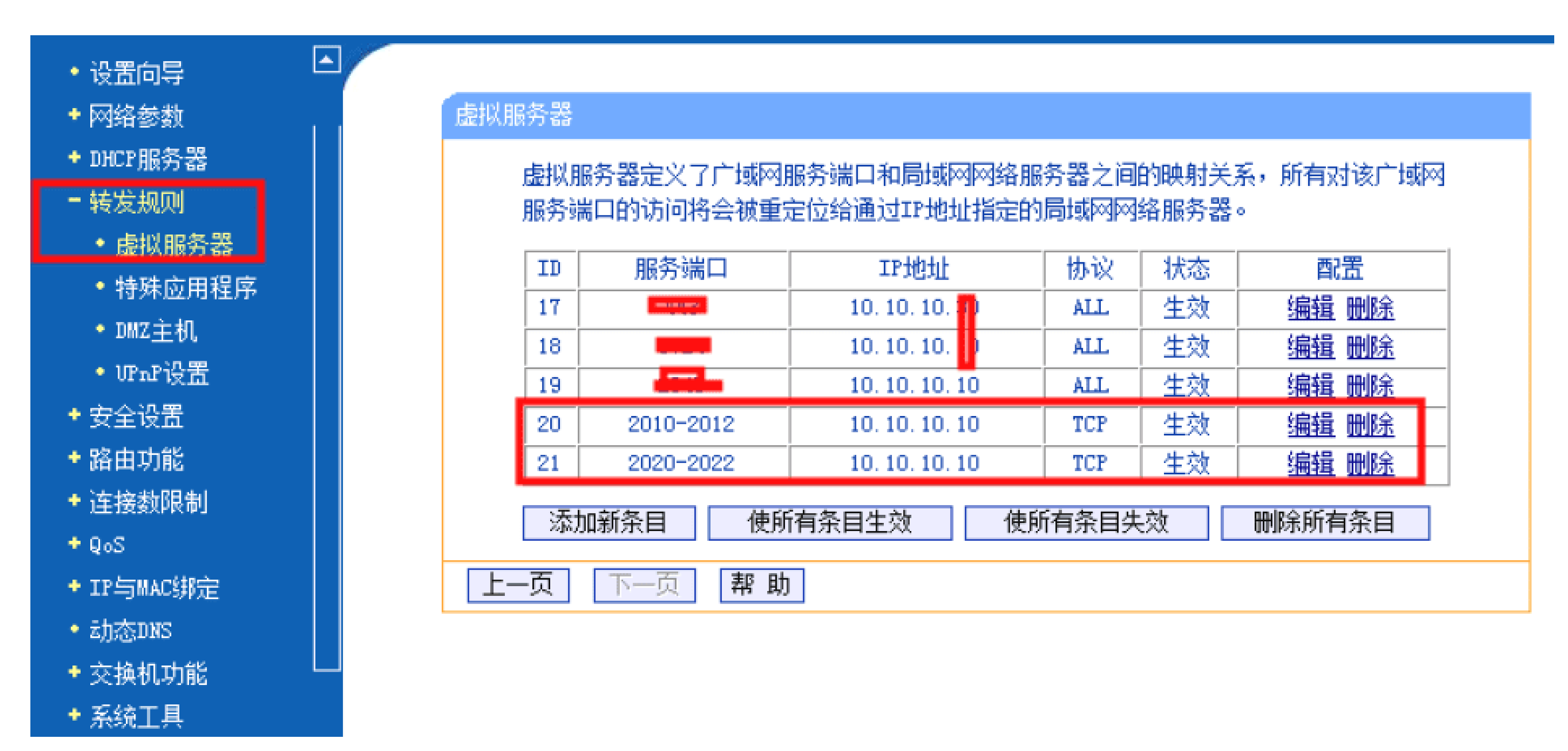


图 5-90 配置双 WAN 口路由器

5.6.3 Forefront TMG 设置

在 Forefront TMG 2010 中，创建两个自定义协议，其中一个协议名称为 FTP_in:2010-2012（也可以是其他名称）、采用 TCP 协议、方向为“入站”、协议号为 2010～2012（如图 5-91 所示）；另一个协议名称为 FTP_in:2020-2022、协议号为 2020～2022 的 TCY 入站协议。然后创建“非 Web 服务器发布规则”，发布 192.168.1.11 的服务器，采用 FTP_in:2010-2012 协议；发布 192.168.1.12 的服务器，采用 FTP_in:2020-2022 协议。

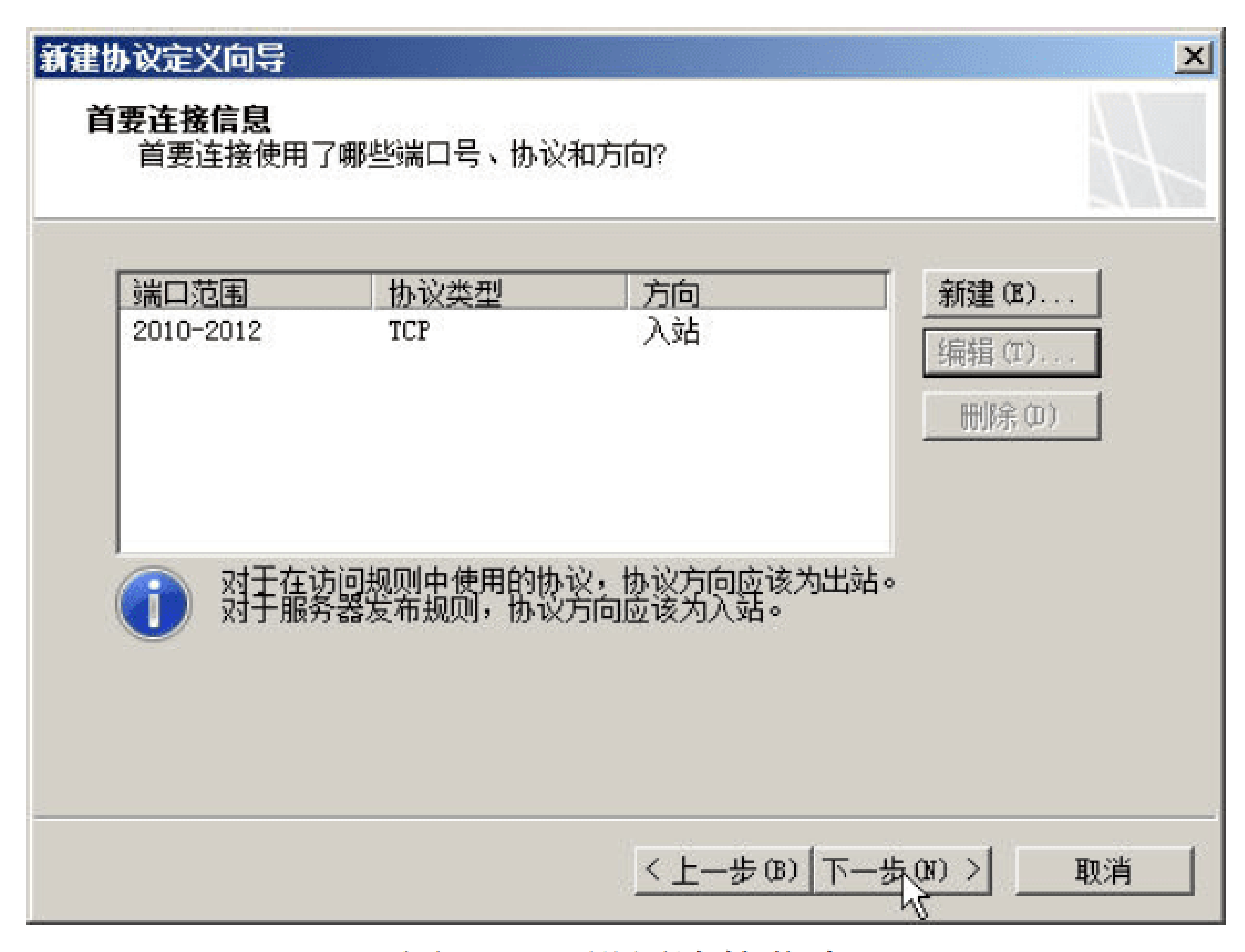


图 5-91　设置连接信息

5.6.4　FTP 服务器设置

在 FTP1 服务器中（已经安装好 Windows Server 2008 R2 协议），安装 IIS 与 FTP 服务，指定 FTP 服务器使用 PASV 的端口为 2012，创建三个 FTP 服务器，这三个服务器可以使用同一个“父目录”，并且这三个服务器的服务端口分别为 21（内网使用）、2010（电信使用）、2011（网通使用）。相关步骤如下。

01 在“Internet 信息服务管理器”中，在 IIS 管理的根路径，双击右侧的“FTP 防火墙支持”链接，如图 5-92 所示。



图 5-92　FTP 防火墙支持

02 在“FTP 防火墙支持”窗格，在“数据通道端口范围”文本框中，输入前面规则的端口范围，在此为 2012-2012，然后单击“应用”按钮，如图 5-93 所示。

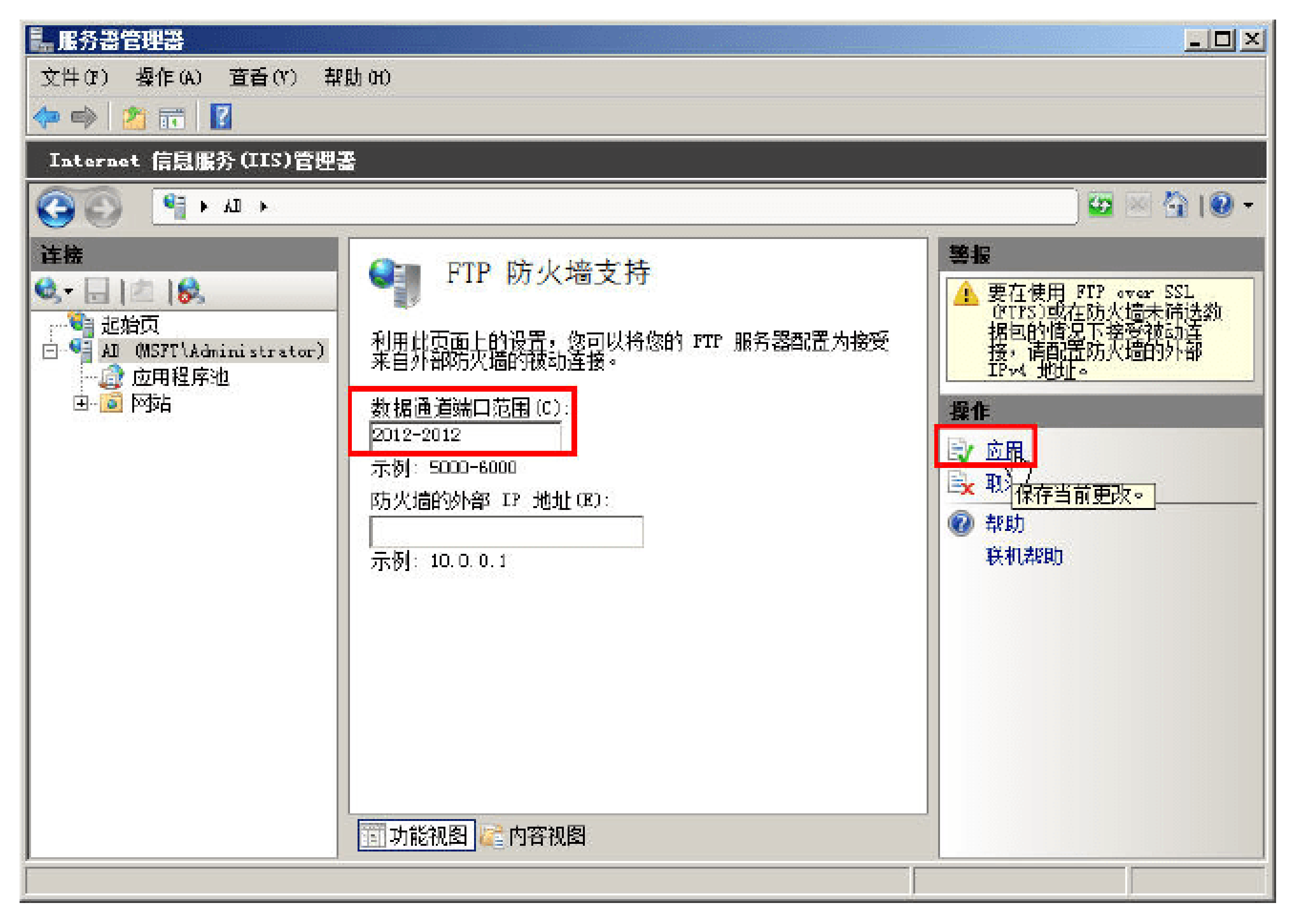


图 5-93　指定 PASV 端口范围

03 返回到图 5-92 后，双击“FTP SSL 设置”链接，选中“允许 SSL 连接”，然后单击“应用”按钮。

接下来创建用于内网使用的 FTP，该 FTP 服务器的端口为 21，步骤如下。

04 右击“网站”，在弹出的快捷菜单中选择“添加 FTP 站点”选项，如图 5-94 所示。也可以单击右侧任务窗格中的“添加 FTP 站点”链接。



图 5-94　添加 FTP 站点

05 设置站点名称为“FTP-21”，并为站点配置物理路径。

06 在“绑定和 SSL 设置”对话框，设置端口号为 21，在“SSL”选项组中，选择“无”。

07 在“身份验证和授权信息”对话框，选择“匿名”用户访问，如图 5-95 所示。

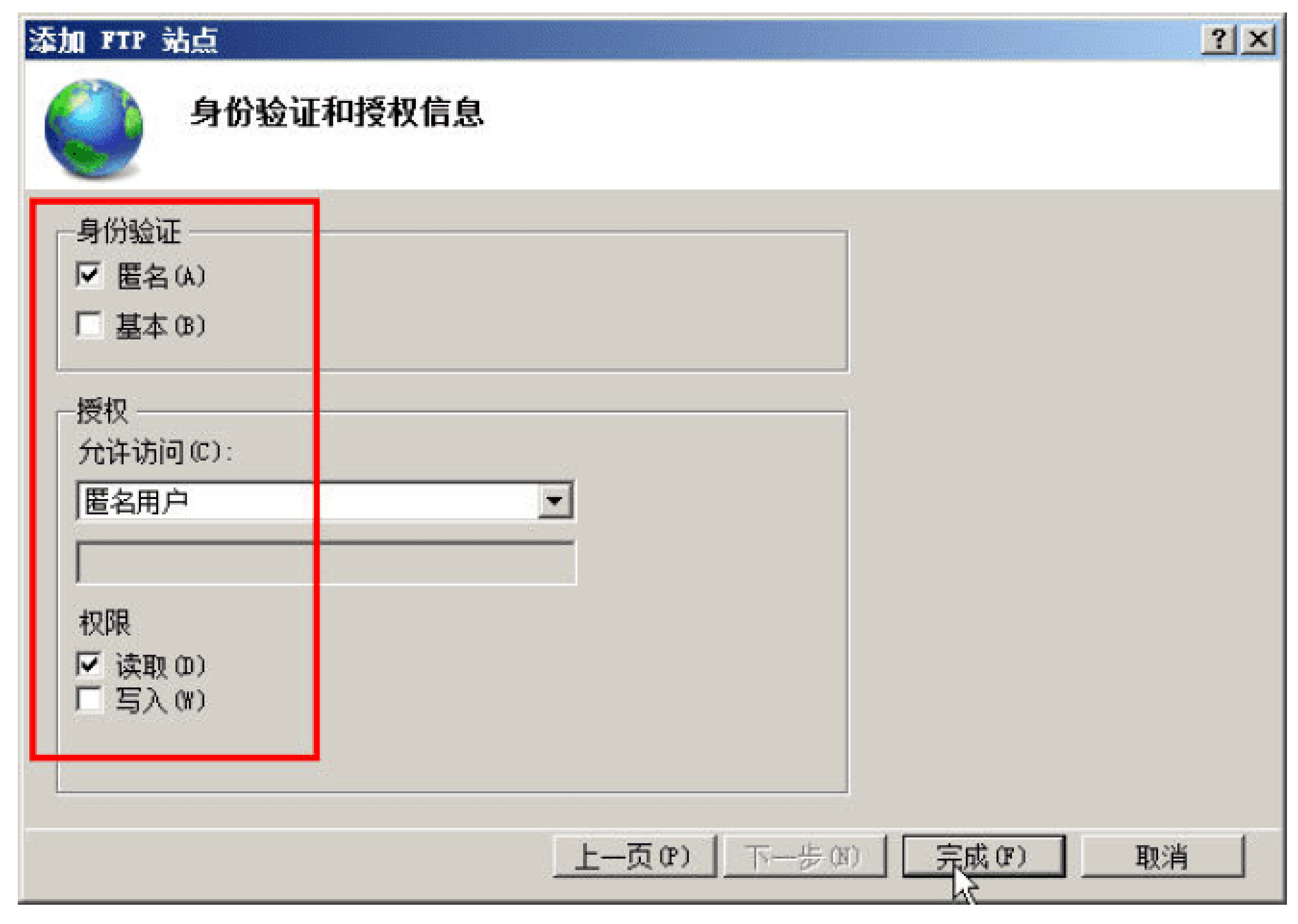


图 5-95　匿名访问

然后参照步骤 4～7，分别创建名为“FTP-DX_2010”、“FTP-WT_2011”的 FTP 站点，使用同一个目录、端口分别为 2010、2011，这些不再一一介绍。

08 创建完成 3 个 FTP 站点后，返回到 IIS 管理器。接下来要修改各 FTP 服务器对外的 PASV 的 IP 地址，以“FTP-DX_2010”站点为例。在 IIS 中，在左侧任务窗格选中“FTP-DX_2010”，双击右侧的“FTP 防火墙支持”链接，如图 5-96 所示。

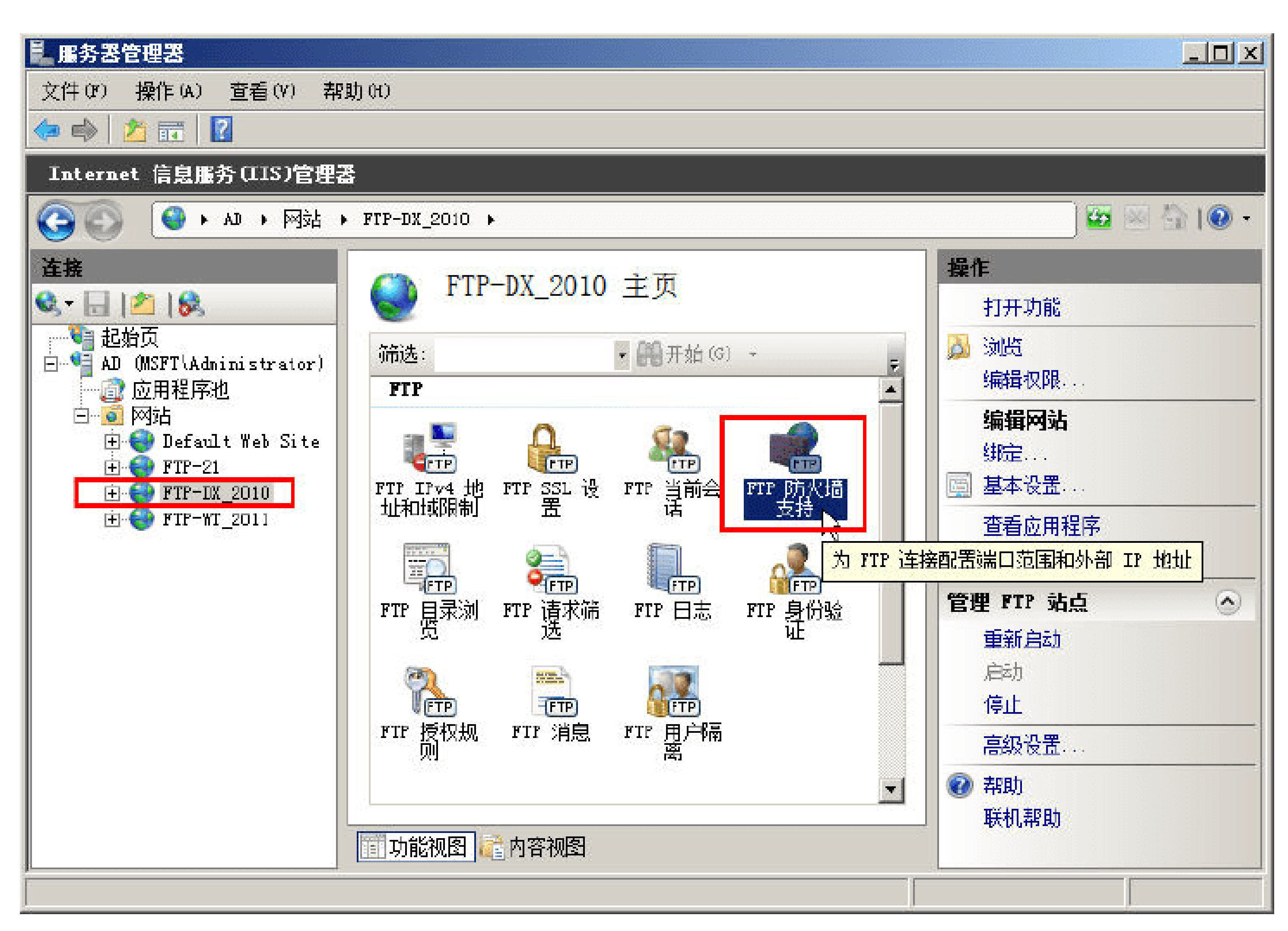


图 5-96　FTP 防火墙支持

在弹出的“FTP 防火墙支持”窗口中，在“防火墙的外部 IP 地址”文本框中，输入外网的 IP 地址，在本例中是 219.x.x.x，然后单击“应用”按钮，如图 5-97 所示。



图 5-97 指定 PASV 的 IP 地址

09 同样，对于发布到网通的“FTP-WT_2011” FTP 站点，修改其 PASV 的 IP 地址为网通的地址，在本例中为 61.y.y.y。

10 而对于用于内网的 FTP，则不需要修改其 PASV 的 IP 地址，该地址为空即可。

经过上述配置，Internet 上的用户以及内网的用户，就可以使用不同的地址与端口访问同一台 FTP 服务器中的内容了。

第 6 章　Windows 系统更新服务器（WSUS）应用

Windows 系统虽然以操作简单、界面友好的特点赢得了广大用户的青睐，但是，层出不穷的漏洞却时时威胁着系统的安全。因此，微软公司也会经常发布各种更新和补丁程序。许多用户除了使用“Windows Update”更新外，还使用“360 安全卫士”或者其他厂商的一些软件进行更新。实际上，360 安全卫士（或者类似的产品）本身并不能提供 Microsoft 产品的更新，他们也是等 Microsoft 发布补丁之后，将补丁的下载地址发给用户，由用户再从 Microsoft 站点下载补丁并进行安装。对于单机用户或者家庭用户来说，使用 360 安全卫士等软件可以减轻用户的负担。但如果是局域网用户，且当网络中计算机数量较多时，大量计算机从 Microsoft 网站下载更新，会占用大量 Internet 带宽。

那么，有没有一种办法，或者有没有这么一种服务器，在局域网中，可以利用网络空闲的时间（例如凌晨时间）自动从 Microsoft 的网站获得更新，而局域网中的计算机在工作时间从局域网的这台服务器获得更新，这样既减少了 Internet 网络带宽的占用，又加快了打补丁的速度呢？WSUS 就是这样一款产品。

6.1　WSUS 3.0 概述与系统需求

WSUS 是 Windows Server Update Services 的简称，是微软推出的网络化补丁分发方案。通过 WSUS，可以集中下载所有的微软产品更新，使客户端可以从 WSUS 服务器快速、方便地下载所需要的更新，而不必连接到微软网站去下载，从而节省带宽、提高效率。WSUS 服务器的特点如下：

- WSUS 是一款免费产品，由 Microsoft 推出。产品的安全性、兼容性毋庸置疑。
- WSUS 对计算机配置的要求不高，只要有足够的硬盘空间即可。
- WSUS 支持 Microsoft 众多的操作系统、应用程序与服务器类产品，例如 Windows XP、Windows Server 2003、Windows 7、Windows Server 2008、Office XP、Office 2003、Office 2007、SQL Server、Exchange 等。
- WSUS 服务器不需要加入到“域”，只要是网络内的一台服务器即可。

客户端采用 WSUS 服务器进行补丁的升级与管理工作，不需要对客户端做过多复杂的设置。如果是域中的工作站，可以用“组策略”统一设置。所有加入到域的计算机都可以自动从 WSUS 服务器升级；没有加入到域的计算机，可以通过导入注册表文件完成设置。

通常情况下，Windows 操作系统从 Microsoft Update 站点或者其他合作站点下载 Microsoft 产品的补丁（如图 6-1 所示），然后手动安装。家庭用户，或者是中小企业用户，大多使用这种方式。但是，如果网络规模较大，计算机数量较多，大量计算机从 Microsoft 网络下载更新，就会占用大量的网络带宽，从而影响其他的网络应用。另外，Windows 补丁并不是一起发布的，可能每隔一段时间发布几次补丁，如果手动下载更新，就会占用管理员和用户很多时间。

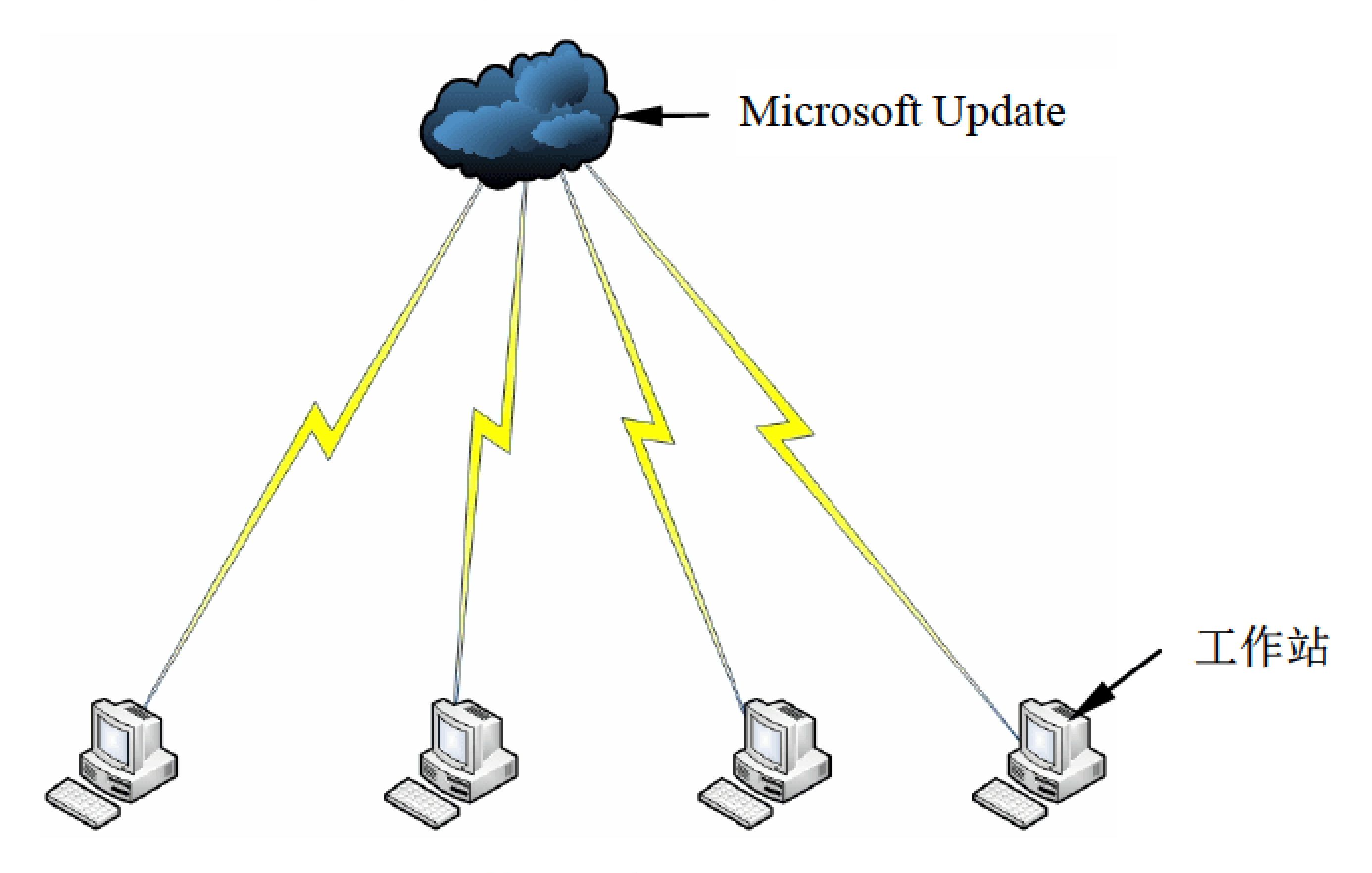


图 6-1　普通用户升级方式

WSUS 是企业内部的升级服务器，它可以从 Microsoft Update 站点下载所有的 Microsoft 更新，而工作站则从 WSUS 服务器上升级（如图 6-2 所示），这样不仅大大减少了带宽的占用，还可以管理工作站使其“自动”升级。

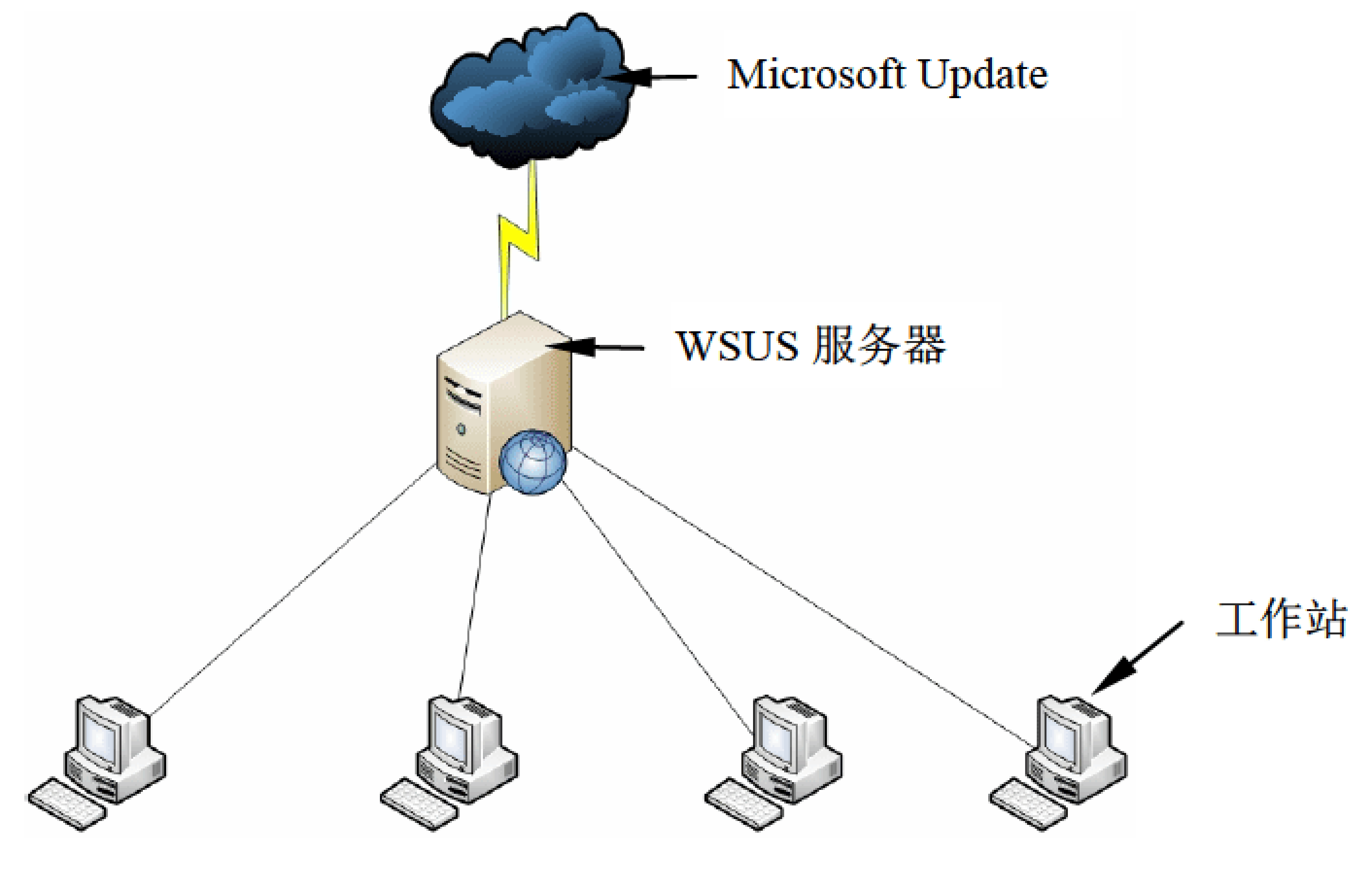


图 6-2　WSUS 体系结构

如果企业网络规模比较大，采用一台 WSUS 服务器不能满足需要，可以采用“多级”WSUS 的体系结构，即为不同网络配置“下游”WSUS 服务器，“下游”WSUS 服务器从“上游”WSUS 服务器下载更新，而“上游”WSUS 服务器直接从 Microsoft Update 站点下载更新，如图 6-3 所示。

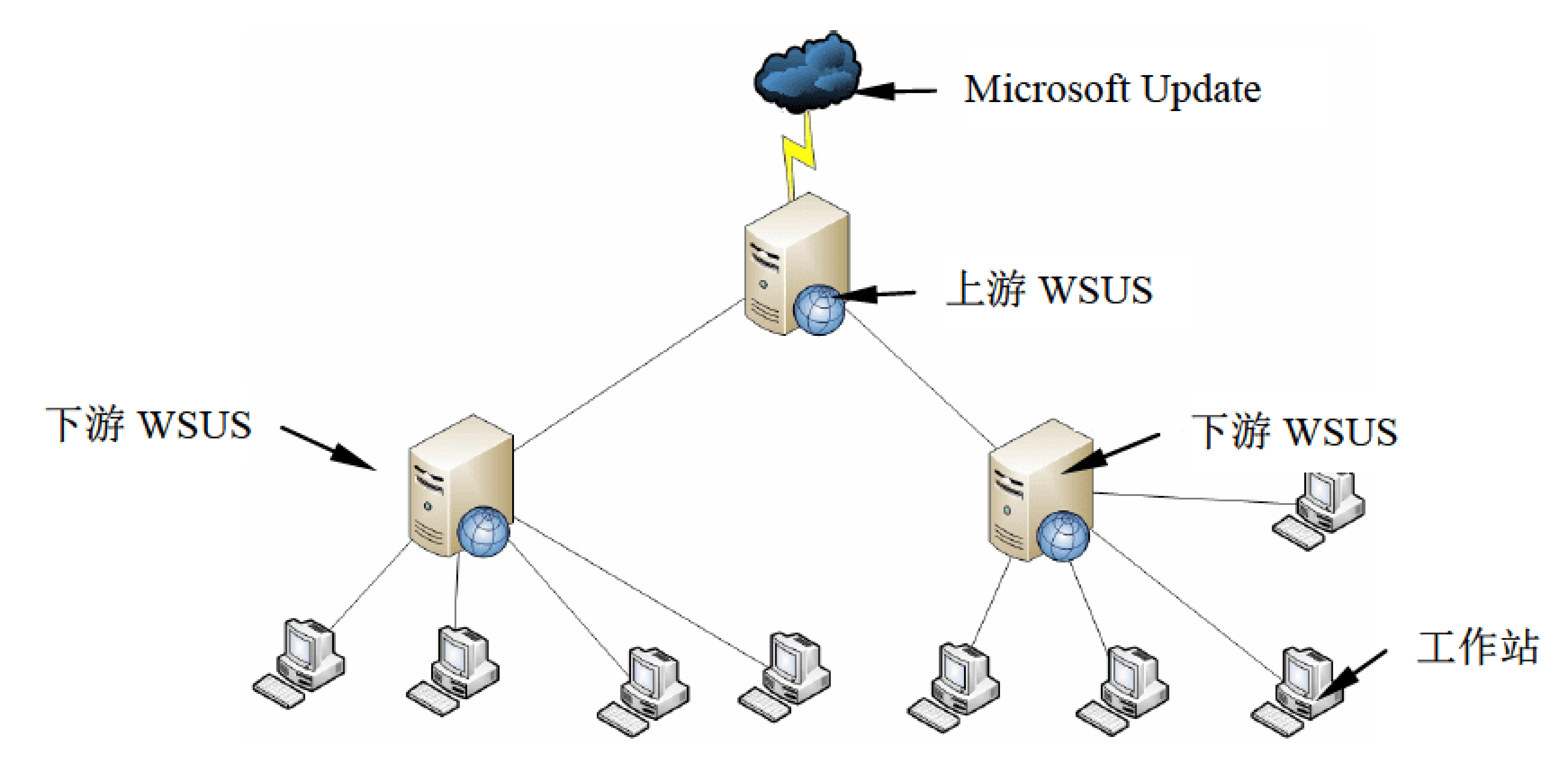


图 6-3 多级 WSUS 体系结构

6.2 WSUS 3.0 的安装与配置

WSUS 3.0 SP1 安装程序可以从如下站点下载：http://www.microsoft.com/downloads/zh-cn/details.aspx?familyid=f87b4c5e-4161-48af-9ff8-a96993c688df&displaylang=zh-cn。

在下载的时候，文件名为“WSUSSetup_30SP1_x64.exe”是 64 位版本，文件名为“WSUSSetup_30SP1_x86.exe”是 32 位版本，请根据自己的服务器操作系统的产品，选择合适的版本。



说 明

（1）在做这个实验的时候，由于 WSUS 服务器需要从 Microsoft 网站下载更新，所以，须保证 Windows 2008 R2 虚拟机可以访问 Internet，且需要根据网络情况，在虚拟机中设置 IP 地址及 DNS。（2）Windows Server 2008 R2 需要下载 64 位的 WSUS。如果你是在 Windows Server 2008 的 32 位版本做实验，请下载 32 位的 WSUS。

6.2.1 安装 WSUS 服务器

WSUS 服务器需要 IIS 与 Microsoft .NET Framework 3.0 的支持，如果要安装 WSUS 服务器，首先需要安装 IIS，主要步骤如下。

01 在“服务器管理器”窗口中，添加“功能”，在“选择功能”对话框中，选中“.Net Framework 3.0 功能”复选框，如图 6-4 所示。

02 在安装完.Net Framework 后，添加“角色”，安装 IIS 服务，至少要选择“静态内容”、“ASP.NET”、“6.0 管理兼容性”、“Windows 身份验证”服务，如图 6-5 所示。

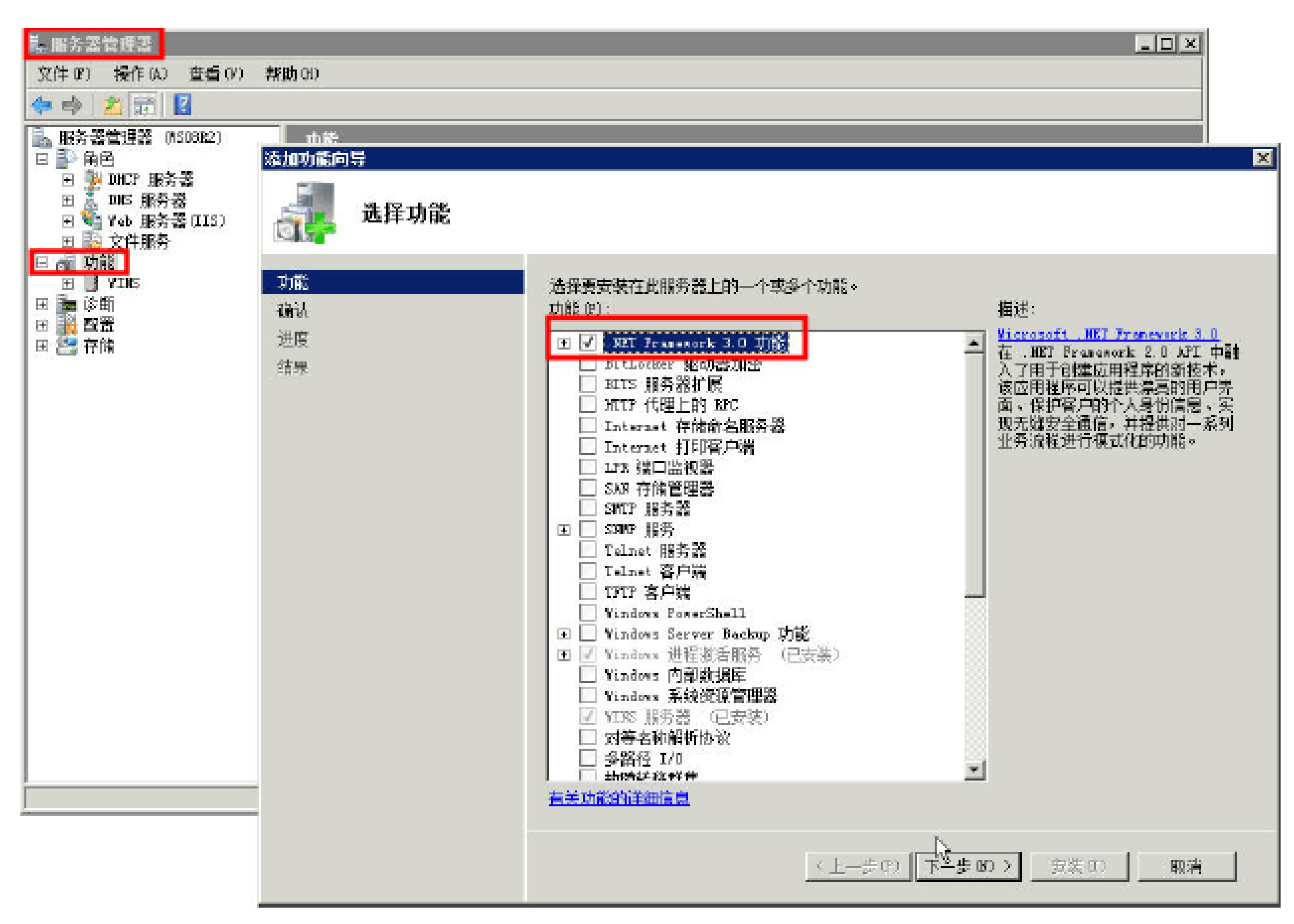


图 6-4　添加.Net Framework 功能

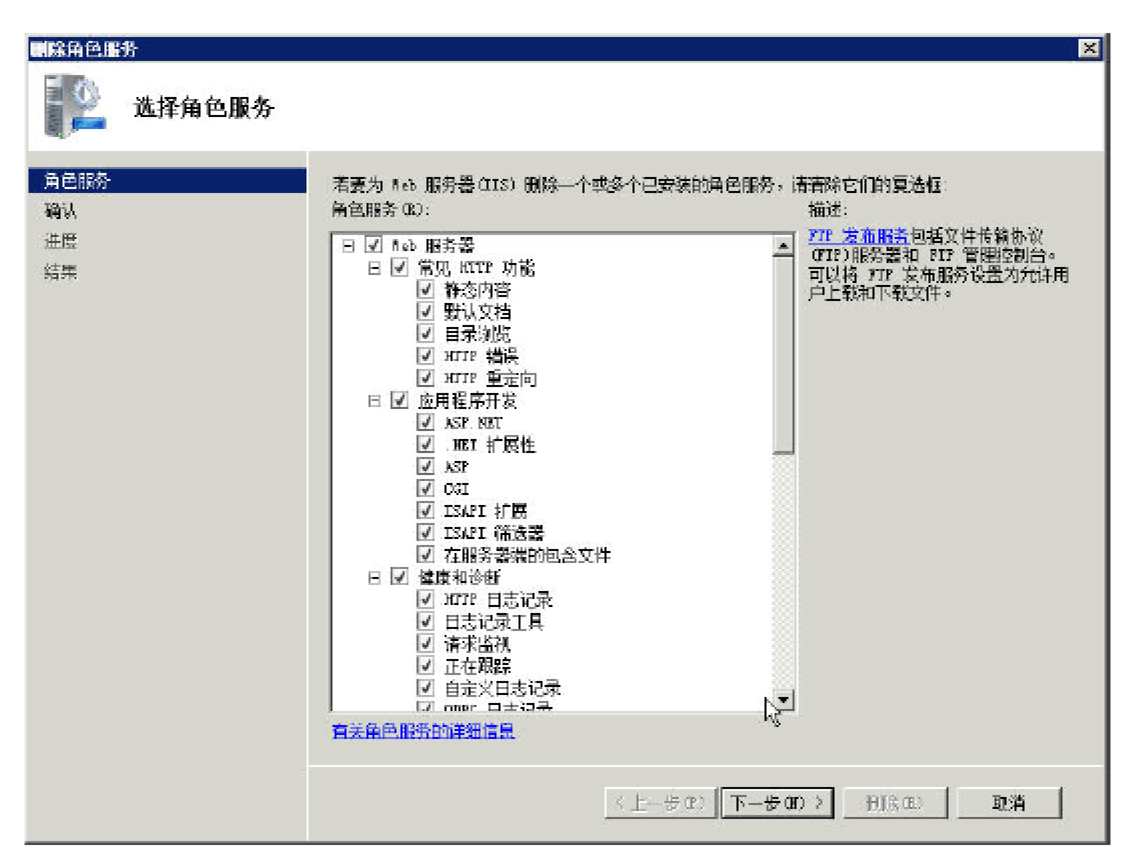


图 6-5　安装 IIS 及其相关角色

在安装完.Net Framework 与 IIS 服务之后，就可以安装 WSUS 3.0 SP1 了，主要步骤如下。

01 运行 WSUS 3.0 的安装程序，进入 WSUS 3.0 SP1 的安装向导，如图 6-6 所示。

02 在“安装模式选择”的对话框中，单击“包括管理控制台的完整服务器安装”单选按钮，然后单击“下一步”按钮，如图 6-7 所示。

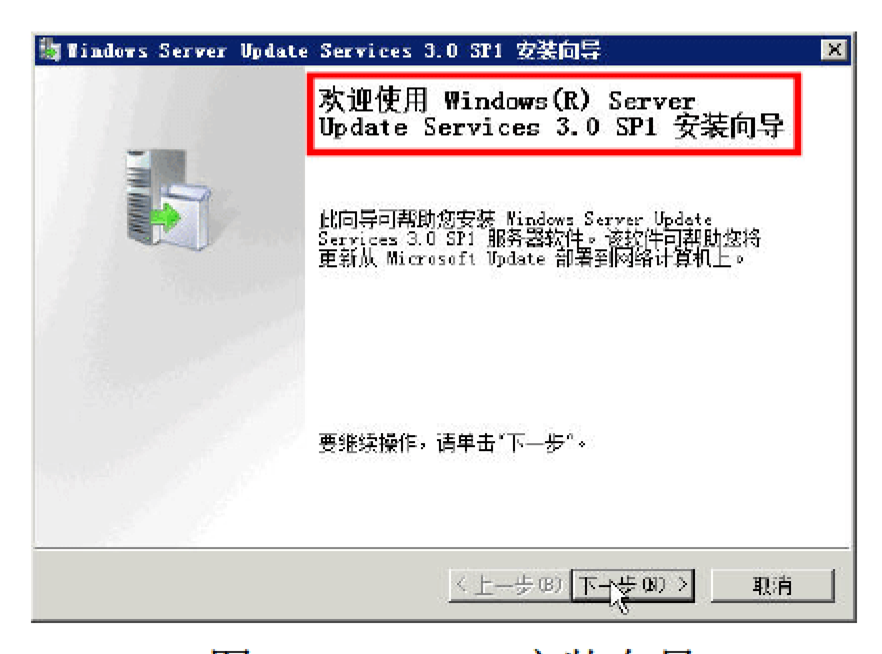


图 6-6　WSUS 安装向导

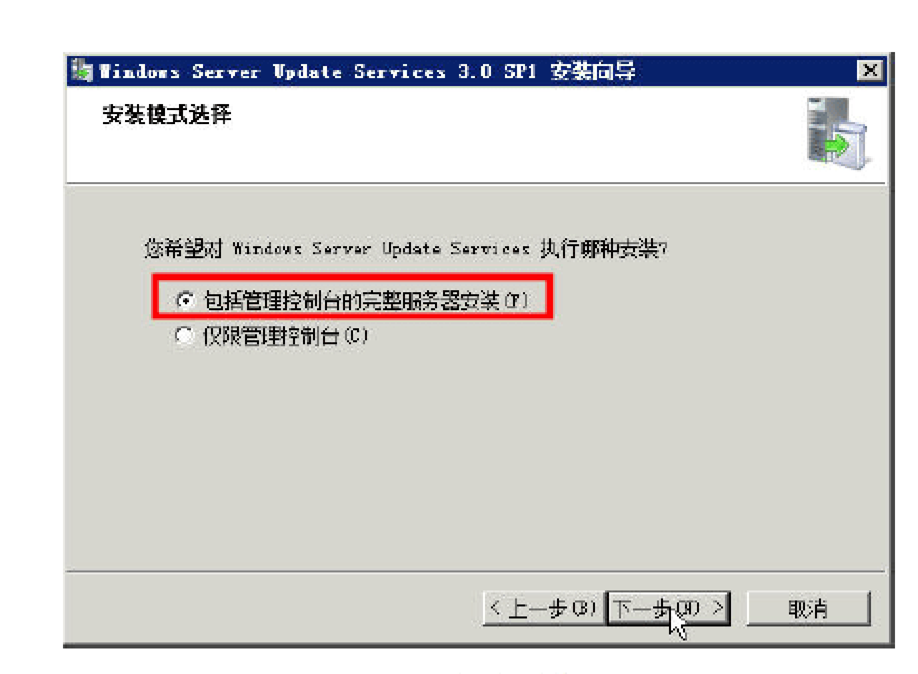


图 6-7　安装模式选择

03 在“许可协议”对话框中选中“我接受许可协议条款”单选按钮，然后单击“下一步”

按钮，如图 6-8 所示。

04 在“使用管理 UI 所需的组件”对话框中，单击“下一步”按钮，如图 6-9 所示。

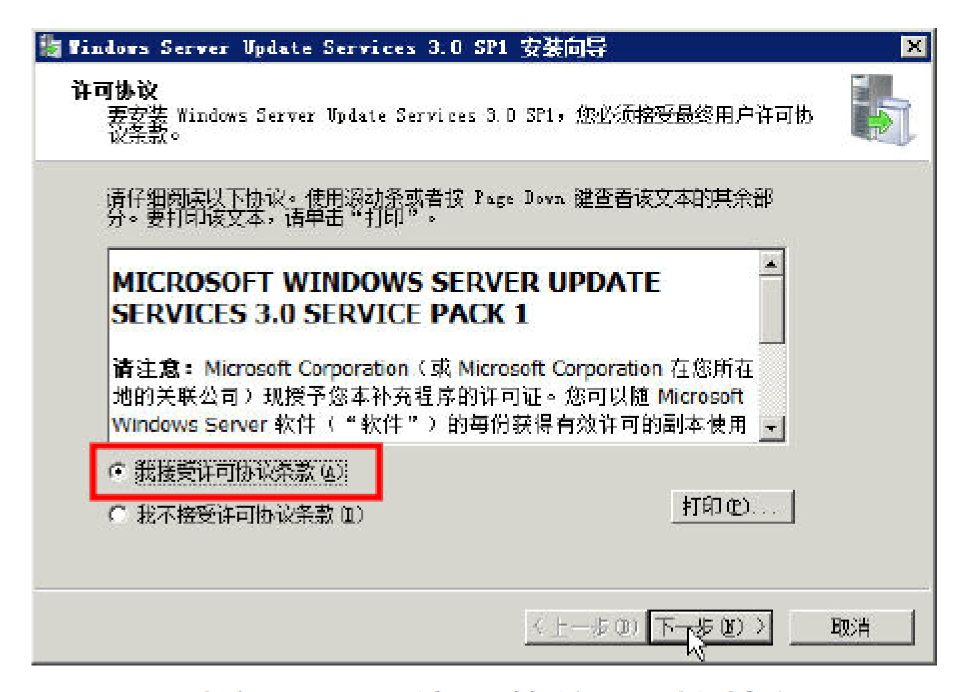


图 6-8　“许可协议”对话框

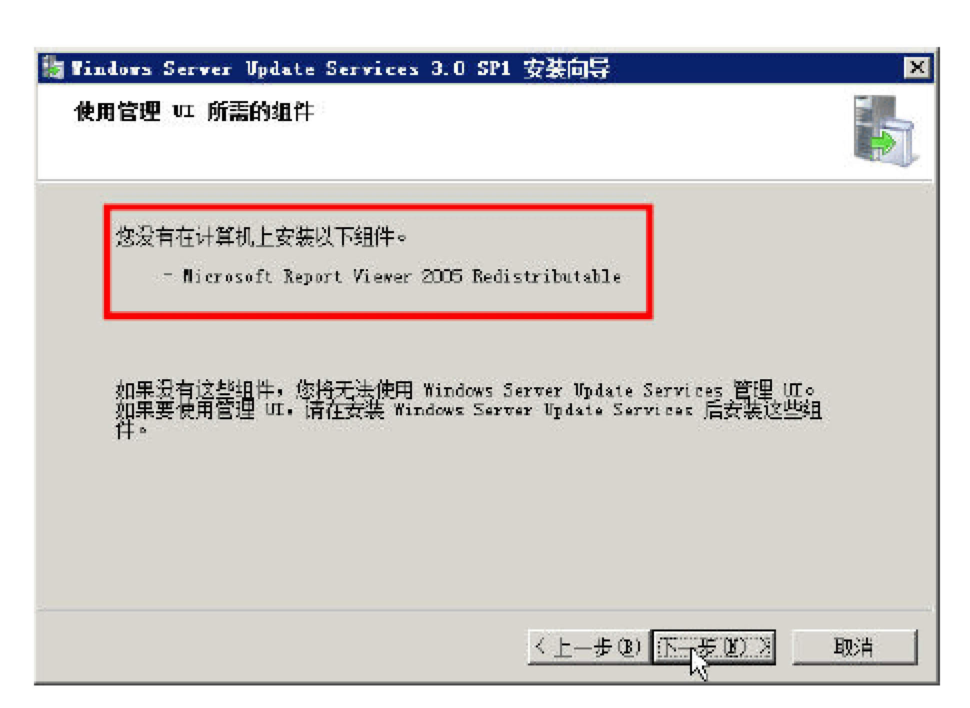


图 6-9　使用管理 UI 所需的组件

05 在“选择更新源”的对话框中，选择保存 WSUS 更新文件的位置，在默认情况下，安装程序会自动选择一个空间最大的分区，并且保存在 WSUS 文件夹中，如图 6-10 所示。

06 在“数据库选项”对话框中，选择保存 WSUS 3.0 数据库的文件位置，如图 6-11 所示。

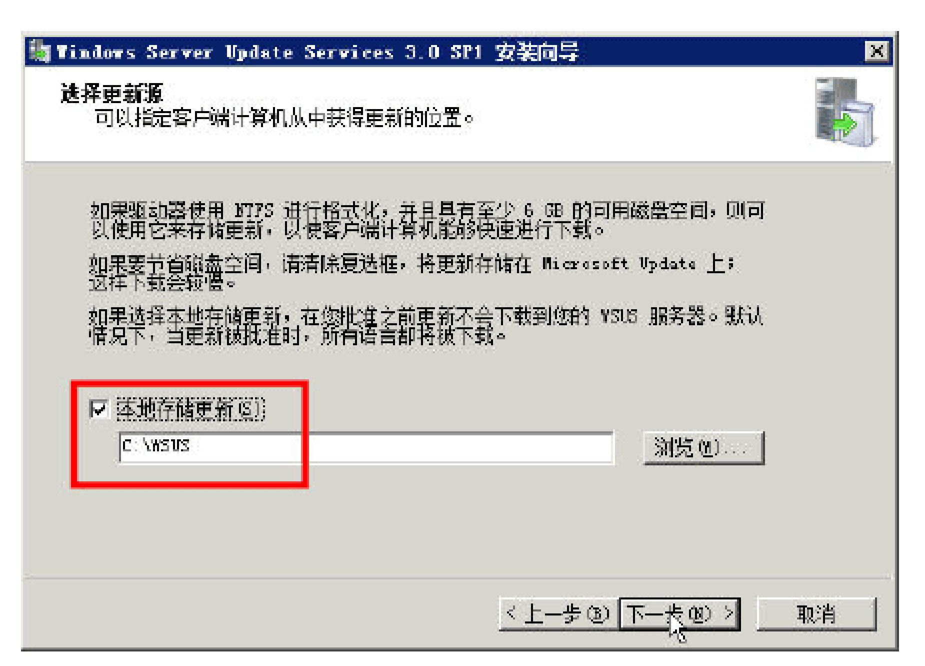


图 6-10　“选择跟新源”对话框

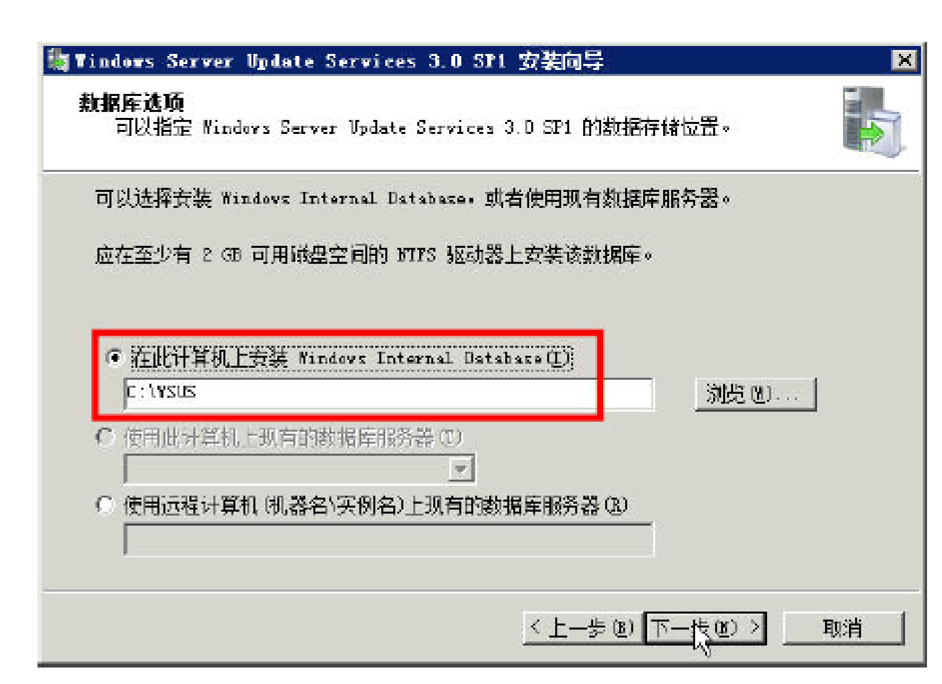


图 6-11　“数据库选择”对话框

07 在“网站选择”对话框中，指定用于 WSUS 3.0 服务的网站。如果安装 WSUS 3.0 的服务器不用做其他用途，可以选择“使用现有 IIS 默认网站”，这样，所有的 WSUS 客户端将使用 TCP 的 80 端口访问和更新补丁，如图 6-12 所示。如果安装 WSUS 3.0 的服务器的 IIS 默认网站有其他用途，可以选择“创建 Windows Server Update Services 3.0 网站”，这样，所有 WSUS 客户端将使用 TCP 的 8530 端口访问和更新补丁，如图 6-13 所示。推荐选择后者，为 WSUS 服务器创建单独的管理网站。

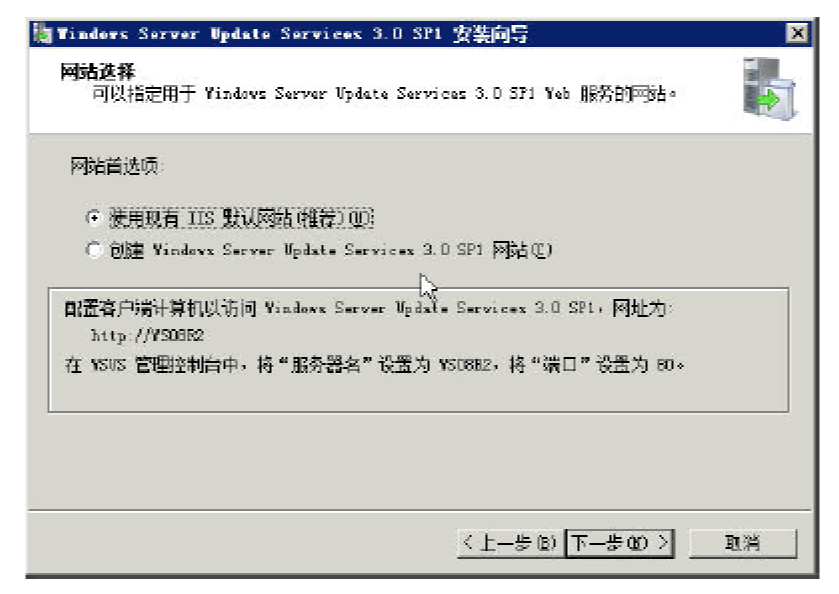


图 6-12　使用默认网站

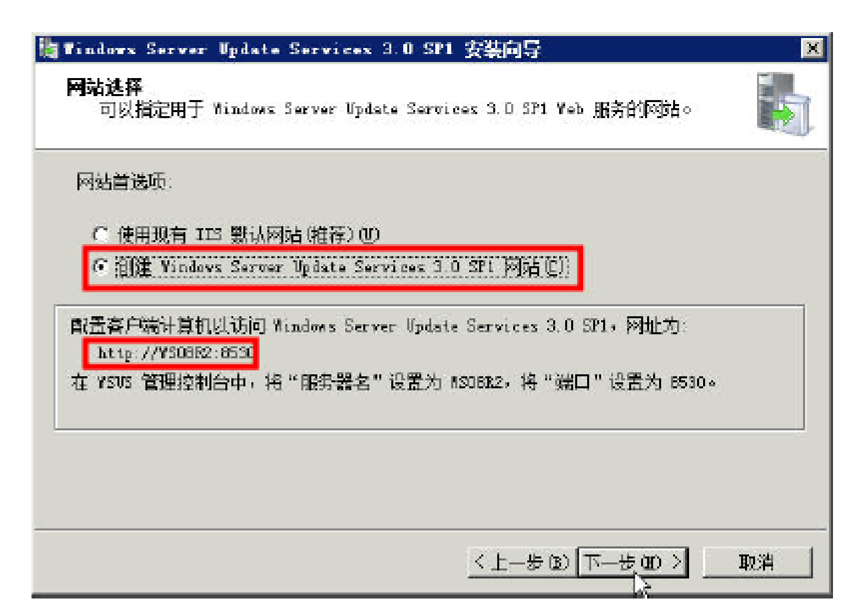


图 6-13　创建网站

08 在“准备安装 Windows Server Update Services 3.0 SP1”对话框中，显示了安装信息，单击“下一步”按钮，如图 6-14 所示。

09 在“正在完成 Windows Server Update Services 3.0 SP1 安装向导”对话框中，单击“完成”按钮，如图 6-15 所示。

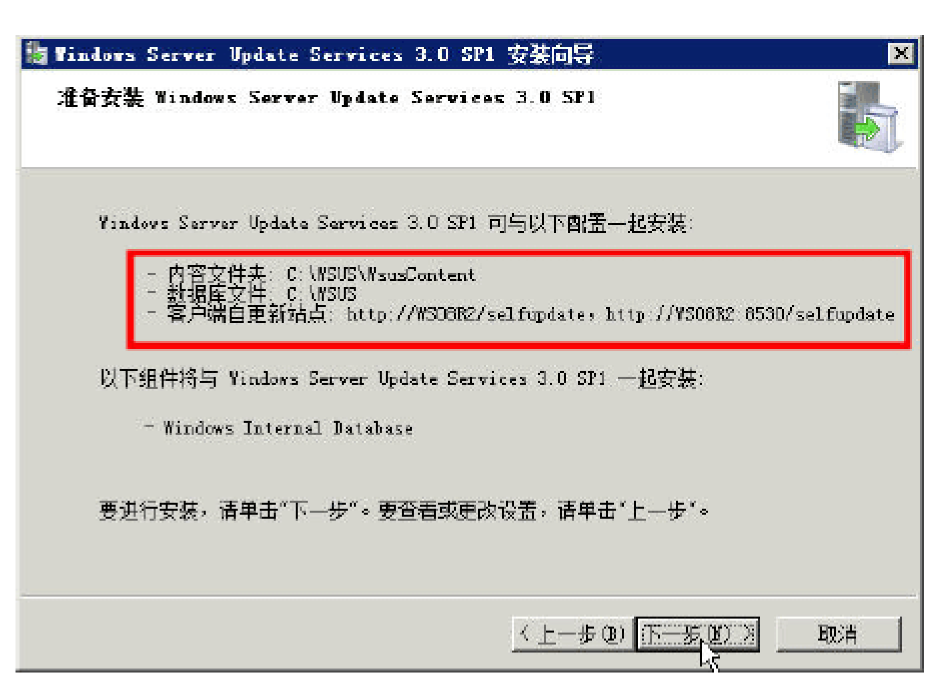


图 6-14　显示安装信息

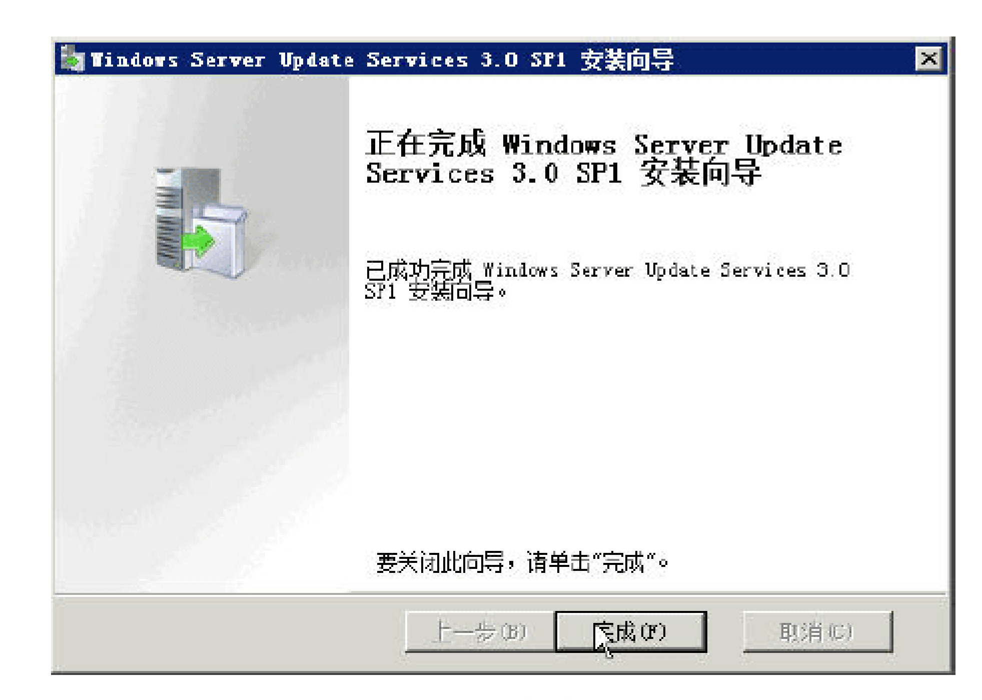


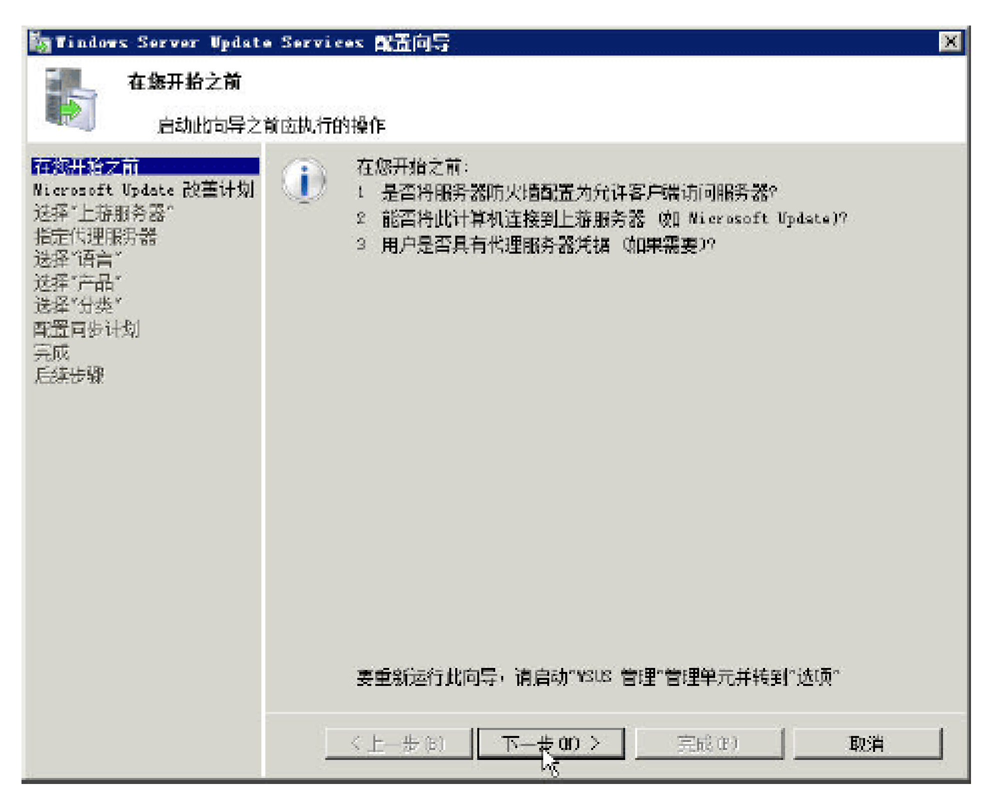
图 6-15　安装完成

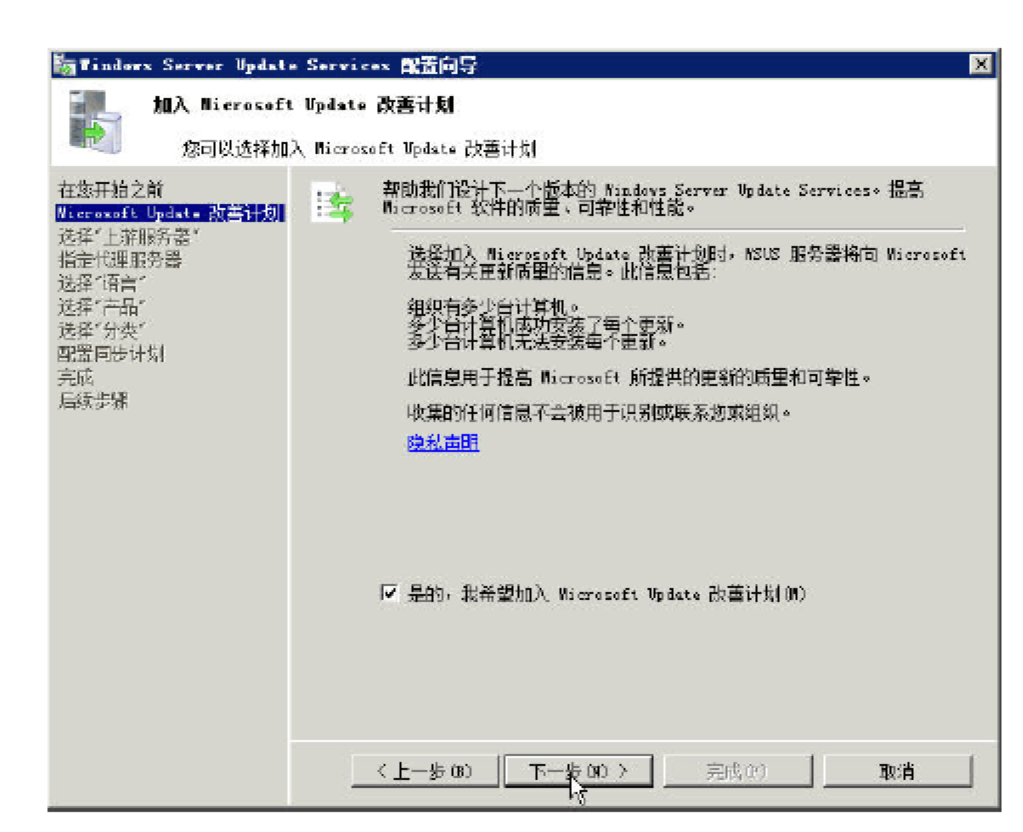
6.2.2　WSUS 3.0 的配置向导

在完成 WSUS 安装之后，首先会进入“Windows Server Update Services 配置向导”界面，接下来将介绍 WSUS 服务器端的配置，步骤如下。

01 在 6.2.1 节图 6-15 中单击“完成”按钮后弹出 “Windows Server Update Services 配置向导”对话框，“在您开始之前”窗口中（如图 6-16 所示），单击“下一步”按钮。

02 在“加入 Microsoft Update 改善计划”对话框中，根据需要，选择是否加入 Microsoft Update 改善计划，如图 6-17 所示。


图 6-16　配置向导


图 6-17　加入 Microsoft Update 改善计划

不管是否加入“Microsoft Update 改善计划”，都不影响 WSUS 3.0 的使用（本例中加入了 Microsoft Update 改善计划）。

03 在“选择‘上游服务器’”的对话框中，选择当前 WSUS 服务器从中同步的“上游”服务器。如果这是网络中的一台 WSUS 服务器，则选择“从 Microsoft Update 进行同步”，如图 6-18

所示。如果网络中已经存在上游 WSUS 服务器，则选择“从其他 Windows Server Update Services 服务器进行同步”，并且在“服务器名”文本框中，输入上游 WSUS 服务器的 IP 地址或计算机名，在“端口号”文本框中，输入上游 WSUS 服务器的端口号，如图 6-19 所示（本例中采用的是从 Microsoft Update 进行同步）。

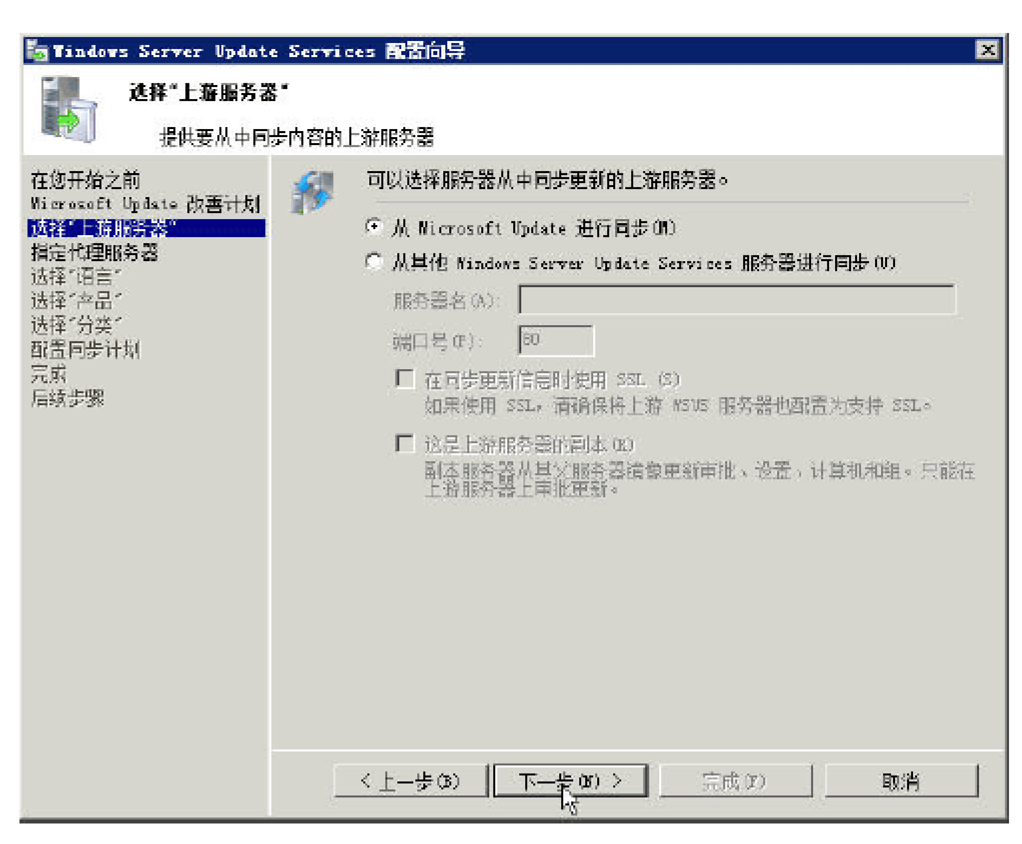


图 6-18　从 Microsoft Update 进行同步

图 6-19　从其他服务器同步

04 在“指定代理服务器”对话框中，设置当前 WSUS 服务器访问 Internet 的方式，如果当前计算机需要使用代理服务器访问 Microsoft Update（或者 WSUS 上游服务器），请选中“在同步是使用代理服务器”复选框并且正确设置代理服务器的参数，如果当前计算机不需要代理服务器，请保持默认值，如图 6-20 所示（本例中未采用代理服务器）。

05 在“连接到上游服务器”对话框中，单击“开始连接”按钮，当前 WSUS 服务器将从 Microsoft Update（如图 6-21 所示）或者上游服务器获得更新信息。

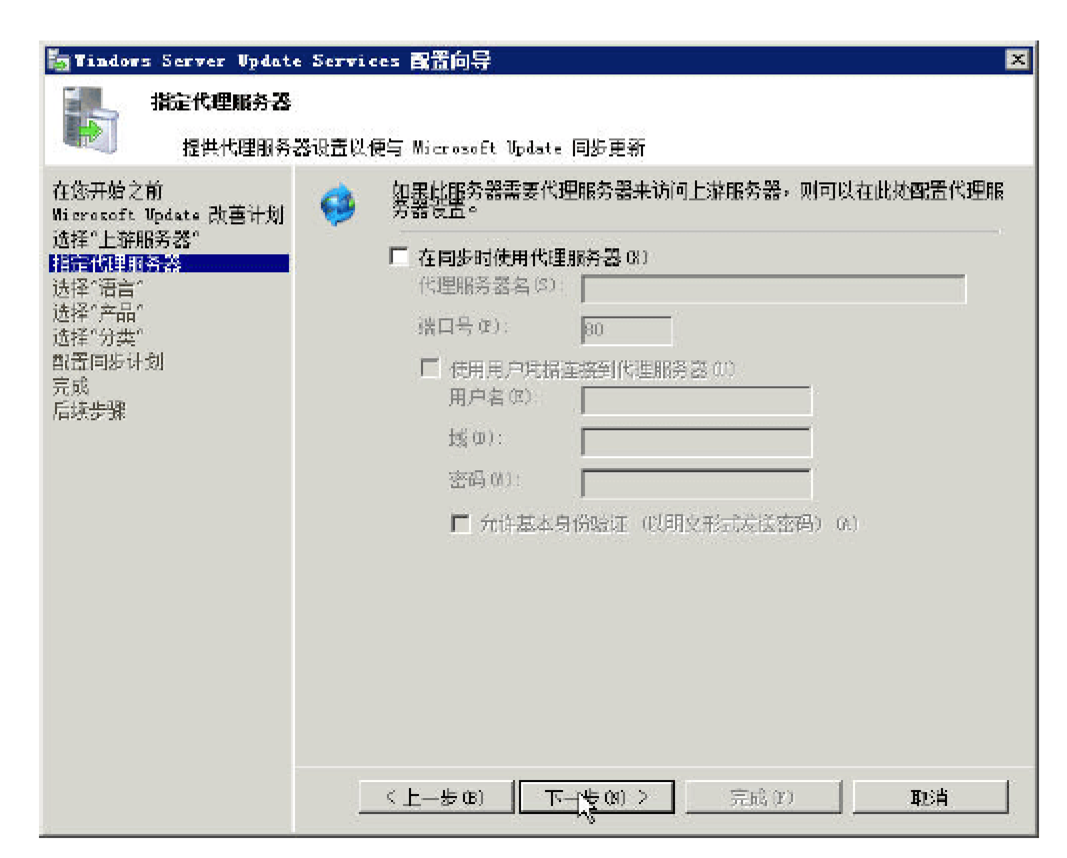


图 6-20　指定代理服务器

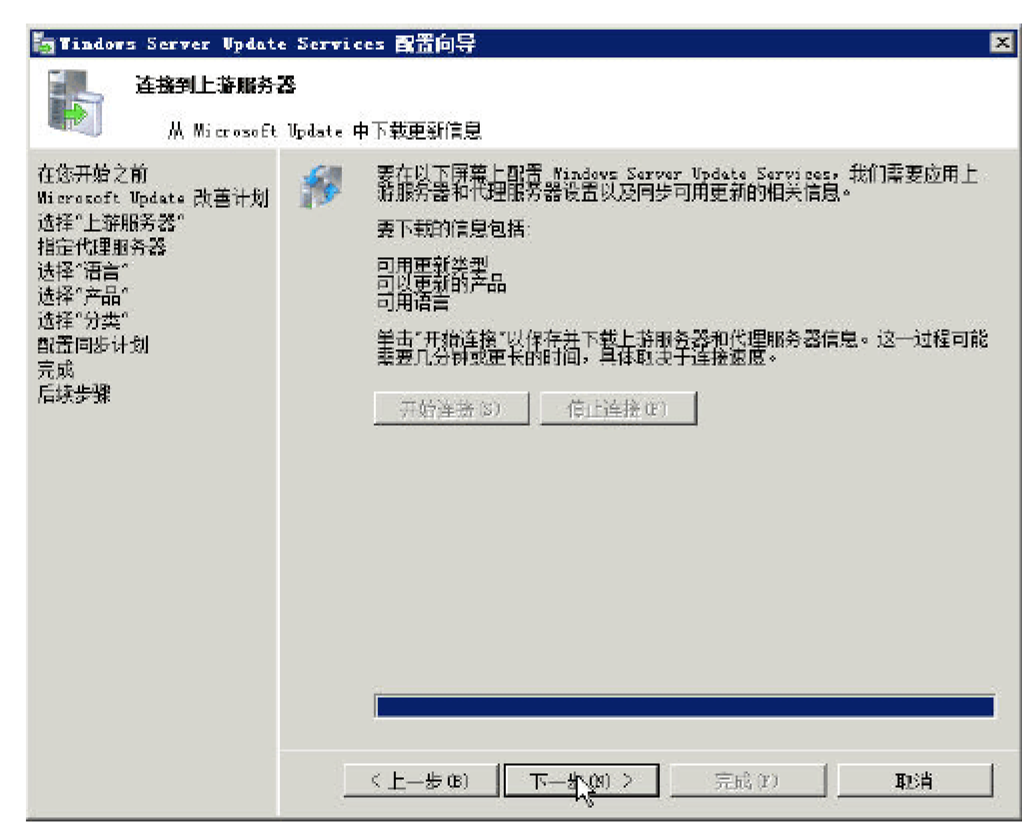


图 6-21　连接 Microsoft Update

连接完成后，单击“下一步”按钮。

06 在“选择‘语言’”对话框中，选择所需语言（默认情况下，选择当前服务器使用的语言，本例为“中文（简体）”），如图 6-22 所示。如果当前 WSUS 服务器是从上游 WSUS 服务器更新，将显示“下载上游服务器支持的所有语言的更新”或“仅下载这些语言的更新（上游服务器

只支持标有星号的语言）”；如果当前 WSUS 服务器是从“Microsoft Update 更新”，将显示“下载包括更新语言在内的所有语言的更新”或“仅下载这些语言的更新”。通常情况下，只让 WSUS 下载与 WSUS 服务器相同语言的更新即可。

07 在“选择‘产品’”对话框中，选择当前 WSUS 服务器将要下载的产品更新。对于管理员来说，可以根据自己所管理的网络中安装的 Microsoft 操作系统、Server、应用程序等进行选择。在本例中，因为是实验的管理，只选择“Virtual PC”，如图 6-23 所示。

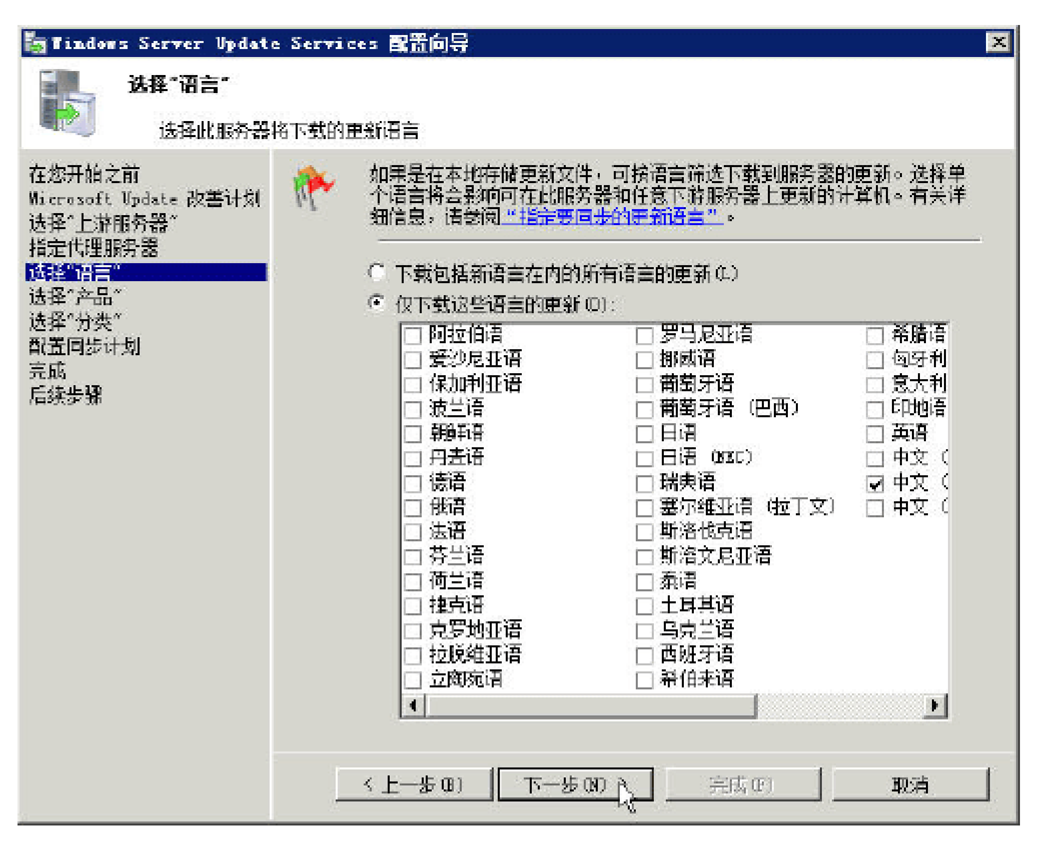


图 6-22　选择语言

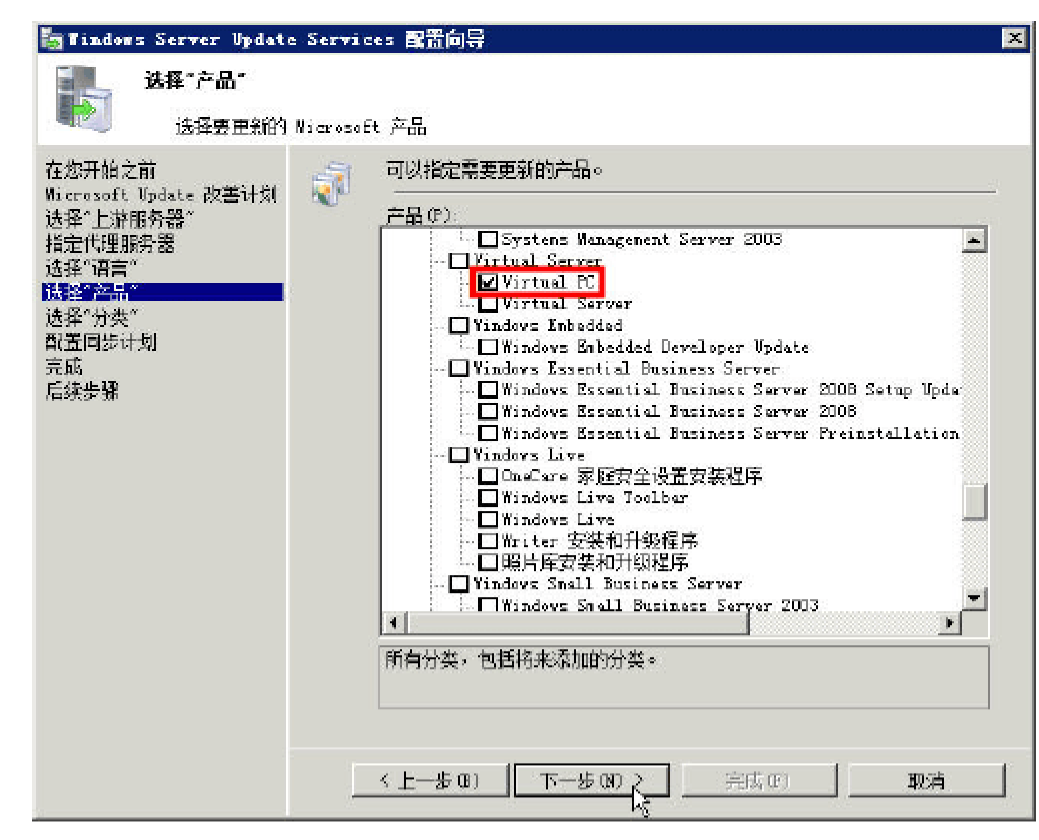
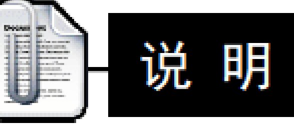


图 6-23　选择产品



说 明

在安装完 WSUS 之后，可以随时根据需要，增加或减少选择更新的 Microsoft 产品。

08 在“选择‘分类’”对话框中，指定要同步的更新分类，如图 6-24 所示

09 在“配置同步计划”对话框中，选择“自动同步”，设定当前 WSUS 服务器与上游 WSUS 服务器同步的方式与同步的时间，通常情况下，选择网络空闲的时间，例如每天的午夜，如图 6-25 所示。

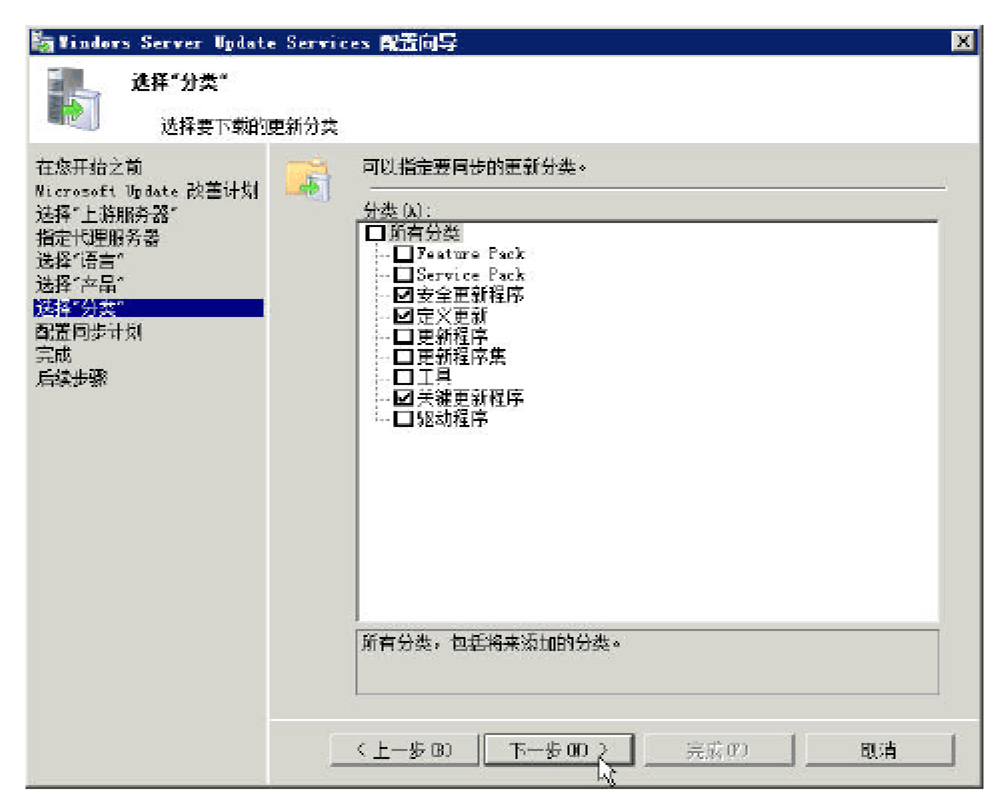


图 6-24　选择产品分类

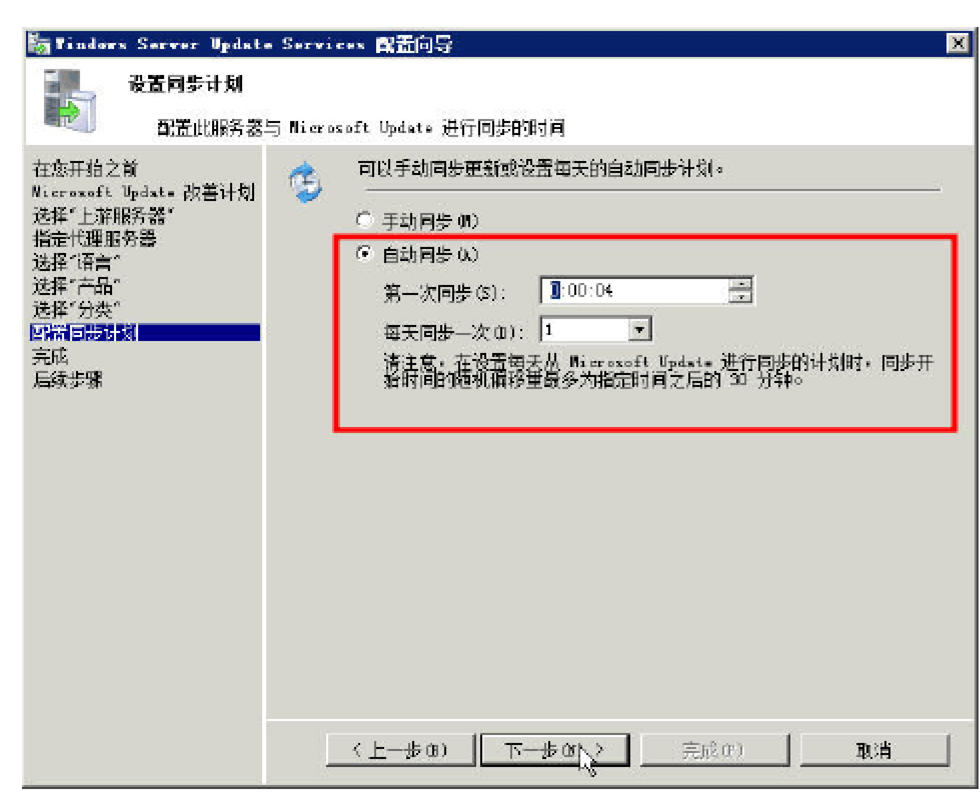


图 6-25　设定同步时间

10 在“完成”对话框中，选中“启动 Windows Server Update Services 管理控制台”复选框，取消“开始初始同步”，如图 6-26 所示。

11 在“后续步骤”中，单击“完成”按钮，完成 WSUS 服务器的配置，如图 6-27 所示。

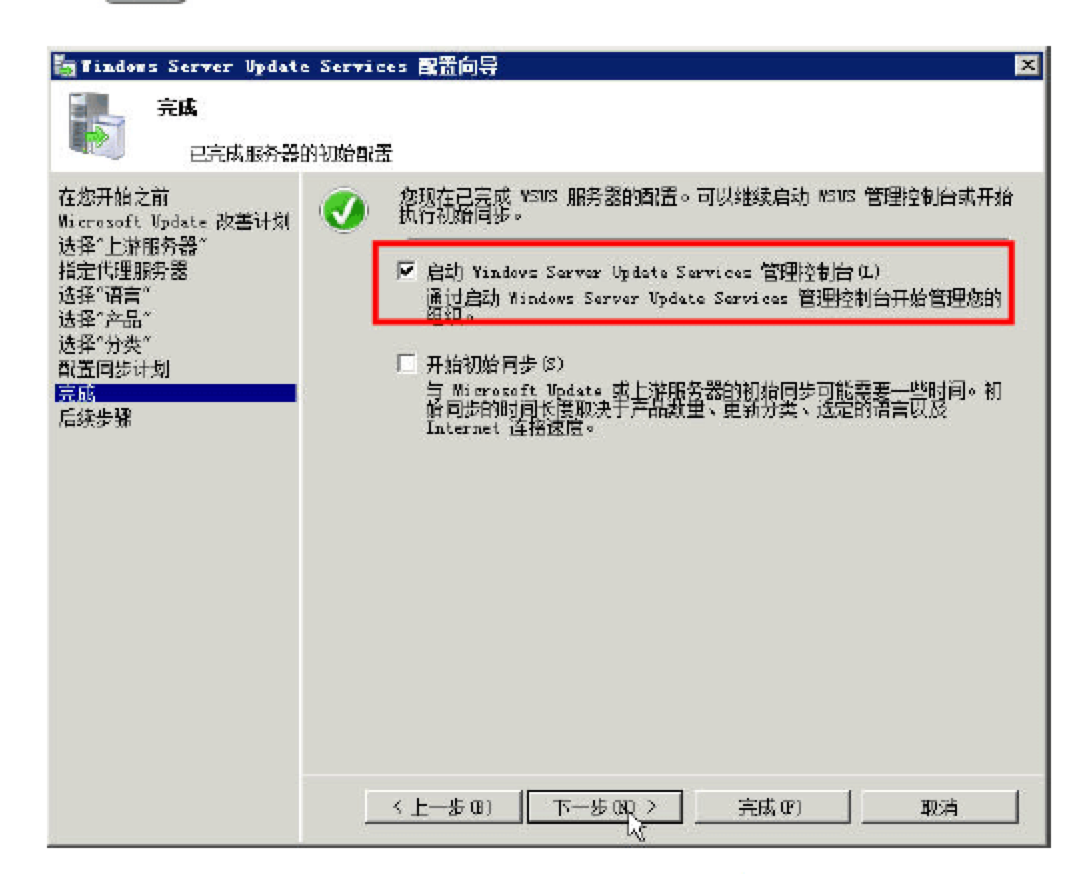


图 6-26　“完成”对话框



图 6-27　完成 WSUS 的配置

WSUS 升级服务器的安装配置已基本完成，下面将介绍 WSUS 服务器的其他配置。

6.2.3　WSUS 服务器自动审批与修改更新配置

为了让 WSUS 服务器“完全自动”地从 Microsoft 的更新服务器获得更新并自动审批，或者用户想要修改 WSUS 的更新配置，可以按照如下的步骤进行操作。

01 从“管理工具”中运行“Microsoft Windows Server Update Services 3.0 SP1”程序，进入 WSUS 管理控制台，在左侧的窗格中选择“选项”，在右侧可以对 WSUS 服务器进行配置。单击“自动审批”链接，如图 6-28 所示。

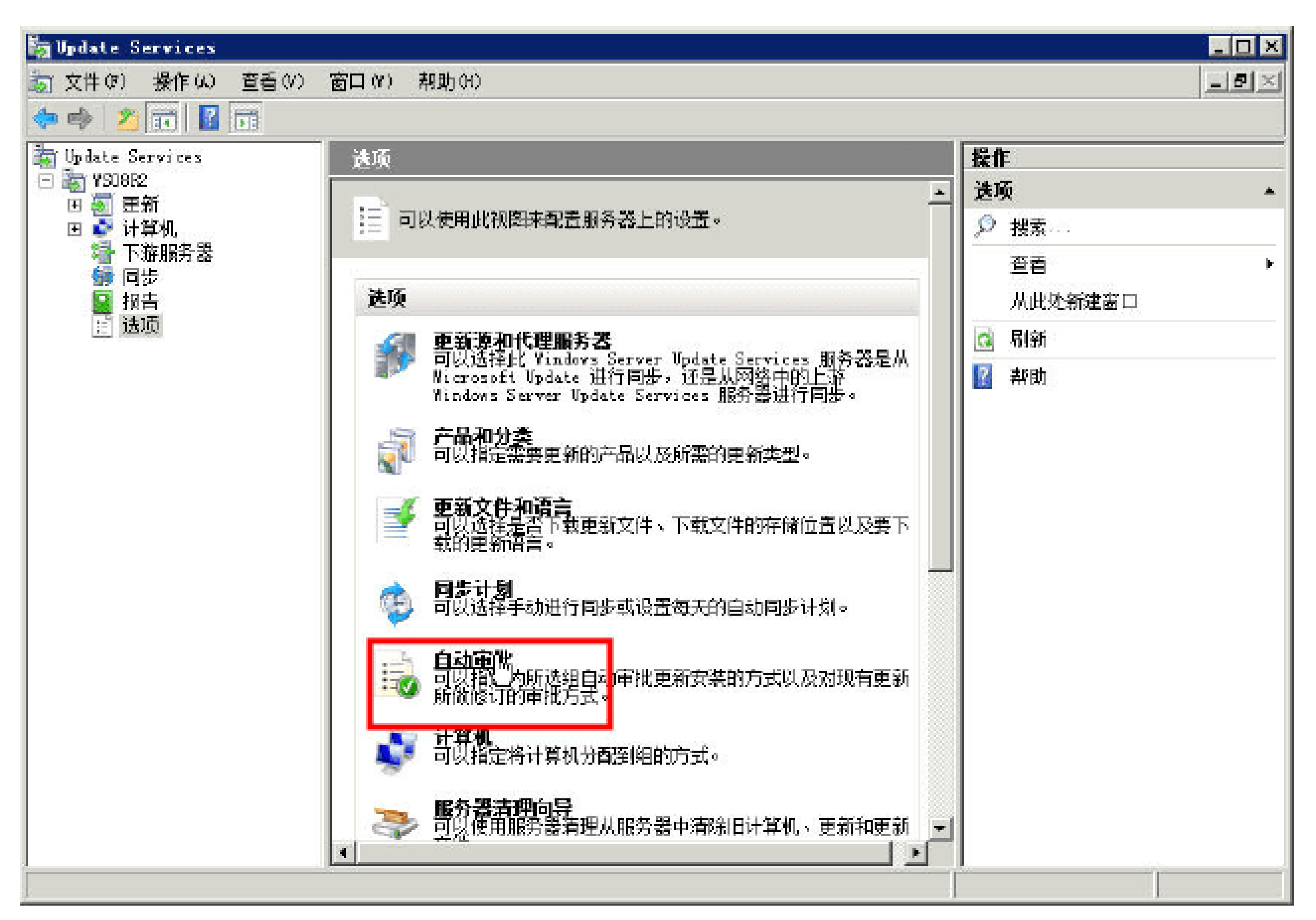


图 6-28　自动审批

02 在“自动审批”对话框中，单击“安全更新程序、关键更新程序”链接（如图 6-29 所示），在弹出的“选择‘更新分类’”对话框中，选中“所有分类”对话框，如图 6-30 所示。

设置完成后，单击“确定”按钮，返回到 WSUS 管理控制台。这样，以后当 WSUS 服务器“上

游更新服务器”或“Microsoft 更新服务器”有更新时，WSUS 服务器将完成“自动审批”的工作。

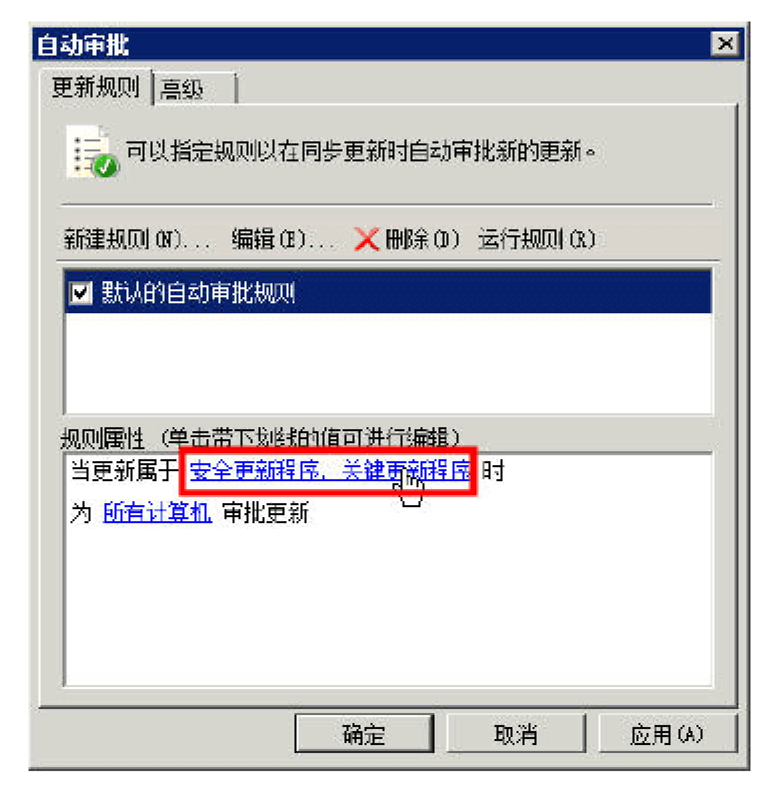


图 6-29　修改自动审批

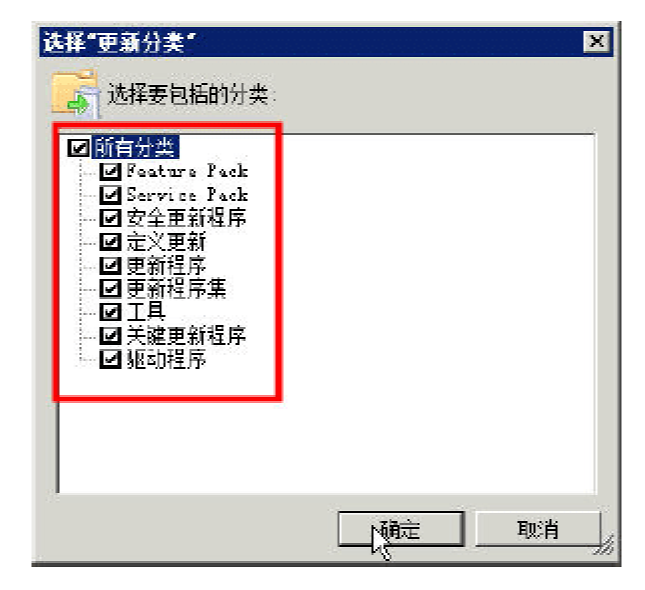


图 6-30　选择所有分类

03 返回到 WSUS 管理控制台后，单击“更新文件和语言”链接，如图 6-31 所示。

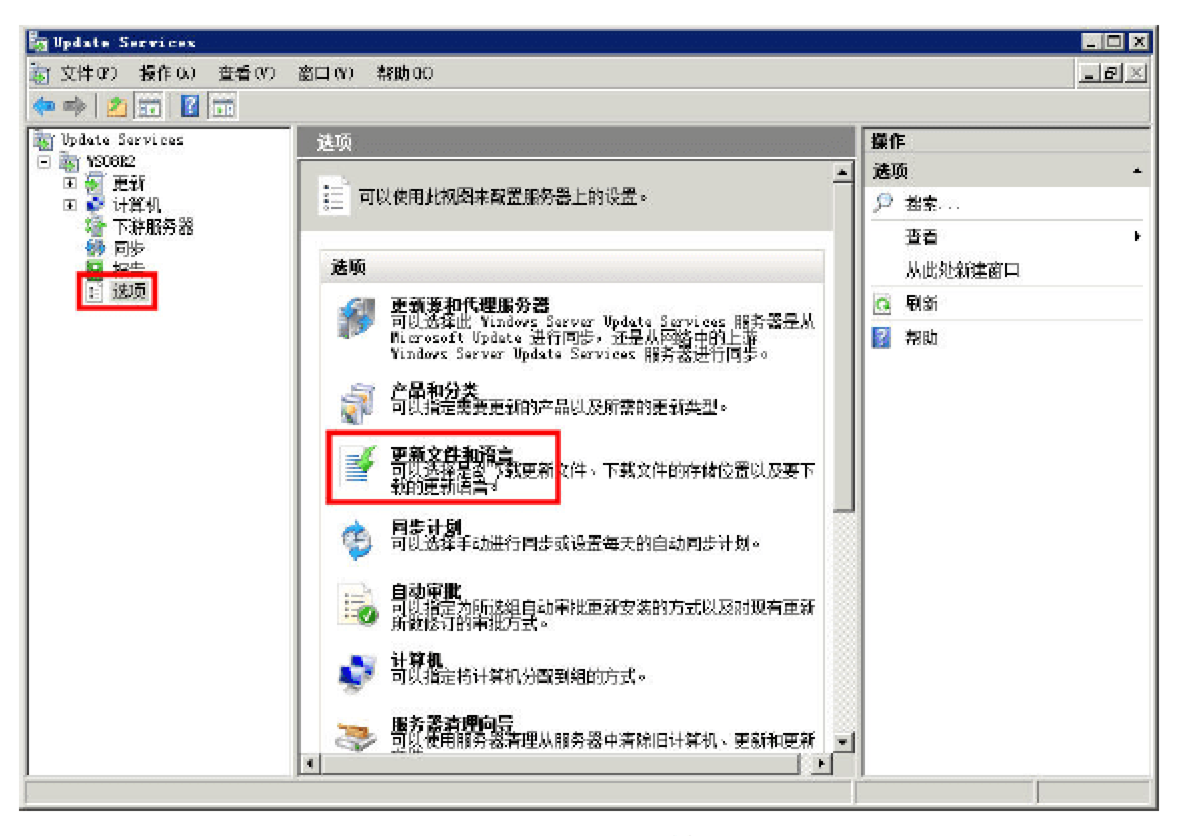


图 6-31　更新文件和语言

04 打开“更新文件和语言”对话框，在“更新文件”选项卡中，选中“下载快速安装文件”复选框，如图 6-32 所示。如果要修改更新语言，可以在“更新语言”选项卡中修改，如图 6-33 所示。

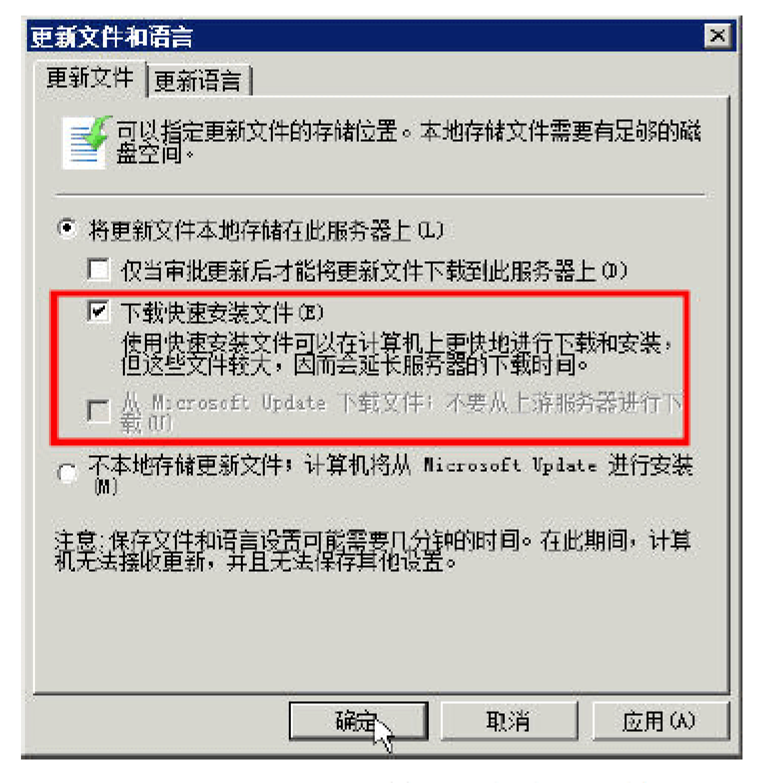


图 6-32　下载快速安装文件

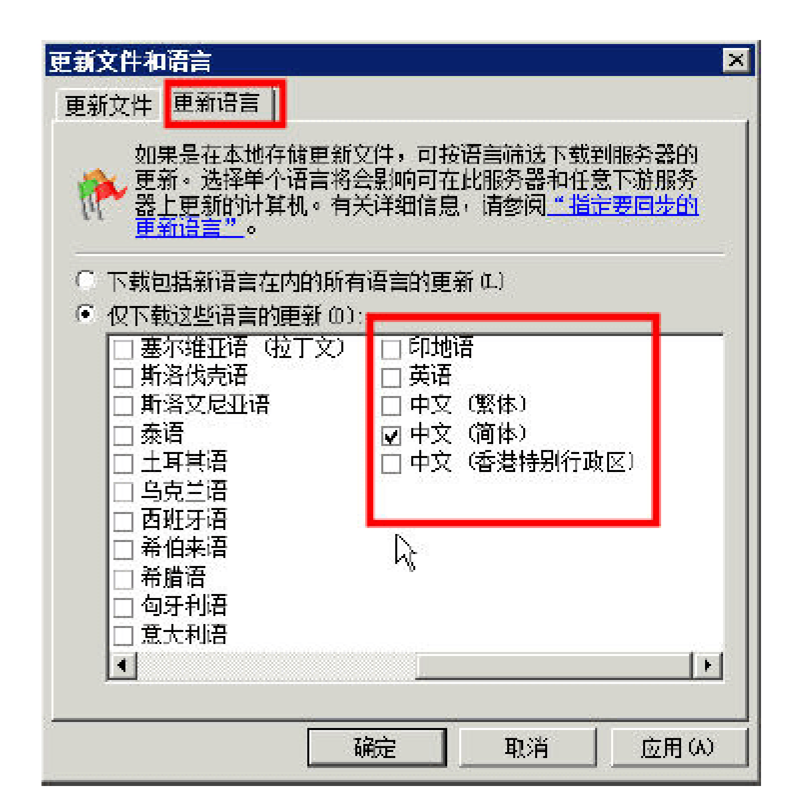


图 6-33　更新语言

05 返回到 WSUS 管理控制台后，单击"产品和分类"链接，打开"产品和分类"对话框，可以在"产品"选项卡中，指定要同步更新的产品（如图 6-34 所示），在"分类"选项卡，指定要同步更新的分类，如图 6-35 所示。

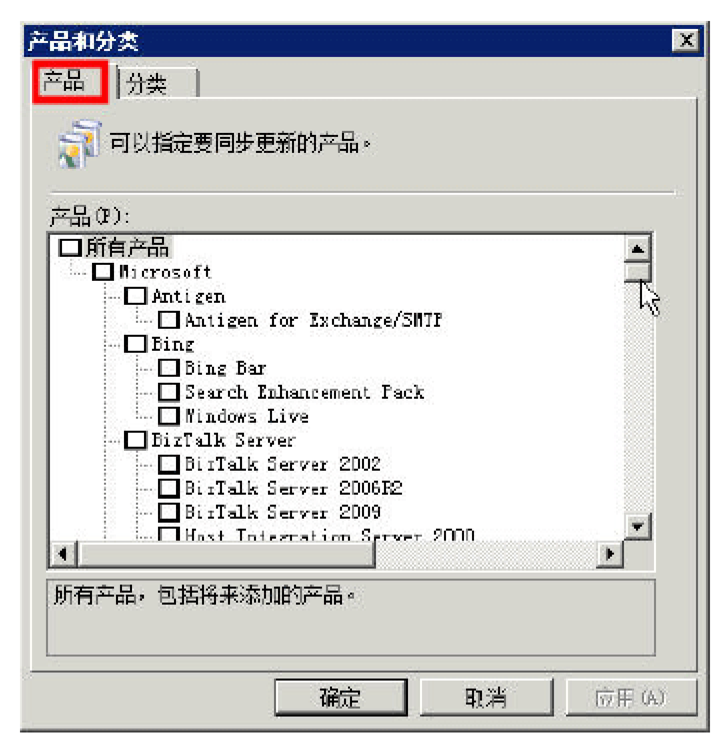


图 6-34　更新产品

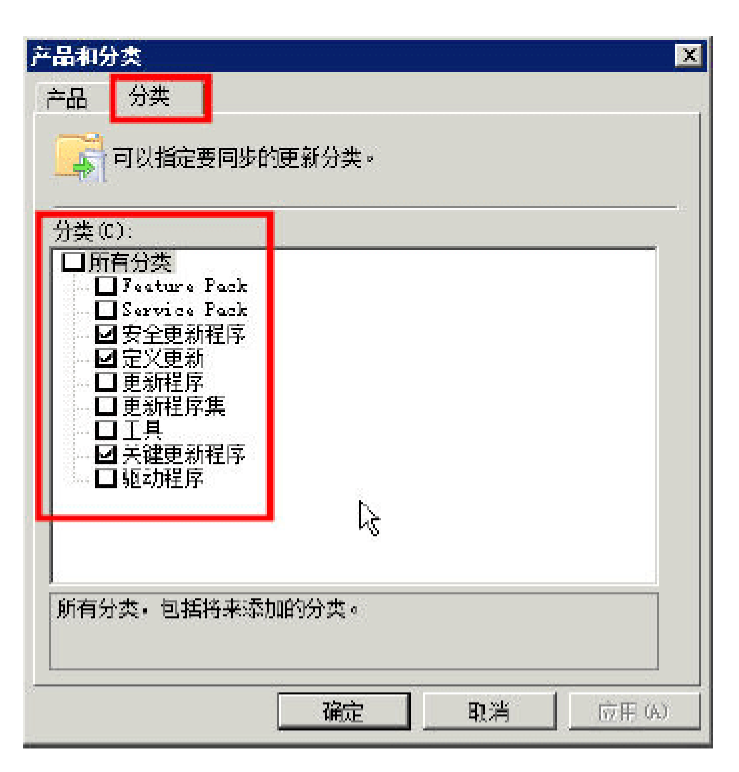


图 6-35　更新分类

06 设置完成后，在左侧任务窗格单击"服务器计算机名"，在右侧单击"立即同步"链接，WSUS 服务器将开始从 Microsoft 更新服务器检索可用的更新并自动下载，如图 6-36 所示。在"同步状态"中显示了同步状态，在"下载状态"中显示了当前需要下载的文件更新数量、已下载更新大小、一共需要下载的更新大小。同时在"连接"处显示了当前 WSUS 服务器的更新端口、服务器版本等。

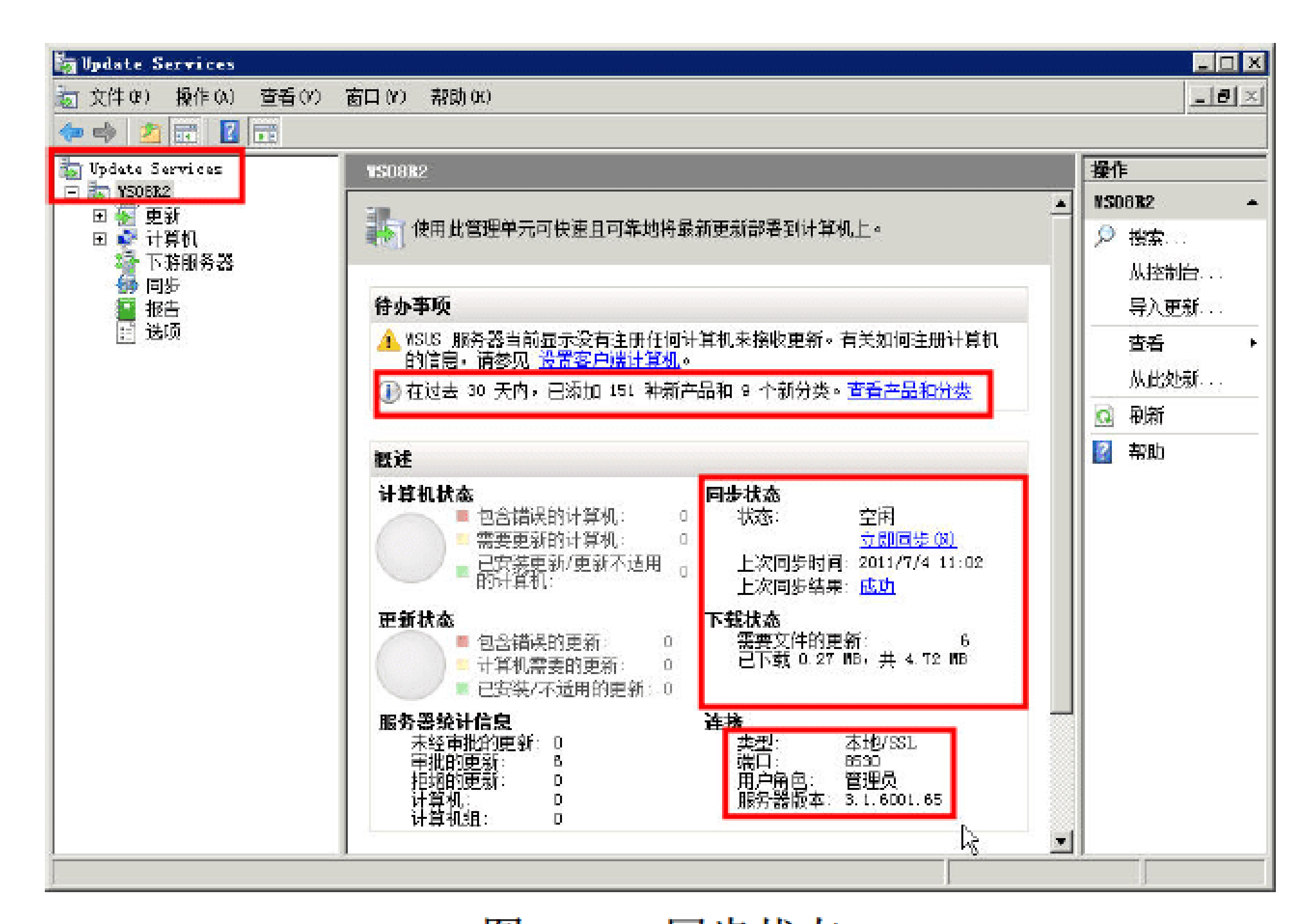


图 6-36　同步状态

6.3　工作站端的配置

由于 WSUS 的目的就是为 Windows 客户端提供更新，因此，任何 Windows 操作系统都可以从 WSUS 服务器下载更新，但需要通过组策略进行配置。

6.3.1 通过本地策略配置客户端

通过组策略或本地策略编辑器配置 WSUS 客户端，是最常用的方法之一。如果是在域环境中，管理员可以通过组策略来集中部署；而工作组中的计算机则需要在每台计算机上修改本地策略使其成为 WSUS 客户端。

下面以 Windows 2000/XP 操作系统为例，介绍通过本地策略配置客户端的步骤，如下所示。

01 以管理员身份登录，依次单击“开始”→“运行”，在“运行”对话框中输入 gpedit.msc 命令。

02 依次展开“计算机配置”→“管理模板”项目，右击“管理模板”并选择快捷菜单中的“添加/删除模板”选项，打开“添加/删除模板”对话框。

03 单击“添加”按钮，在“策略模板”对话框中选择 wuau.adm，如图 6-37 所示。单击“打开”按钮，添加到“添加/删除模板”对话框。

04 单击“关闭”按钮，返回“组策略”窗口。依次展开“管理模板”→“Windows 组件”→“Windows Update”，如图 6-38 所示。此时，即可进行从 WSUS 服务器获取更新的配置。

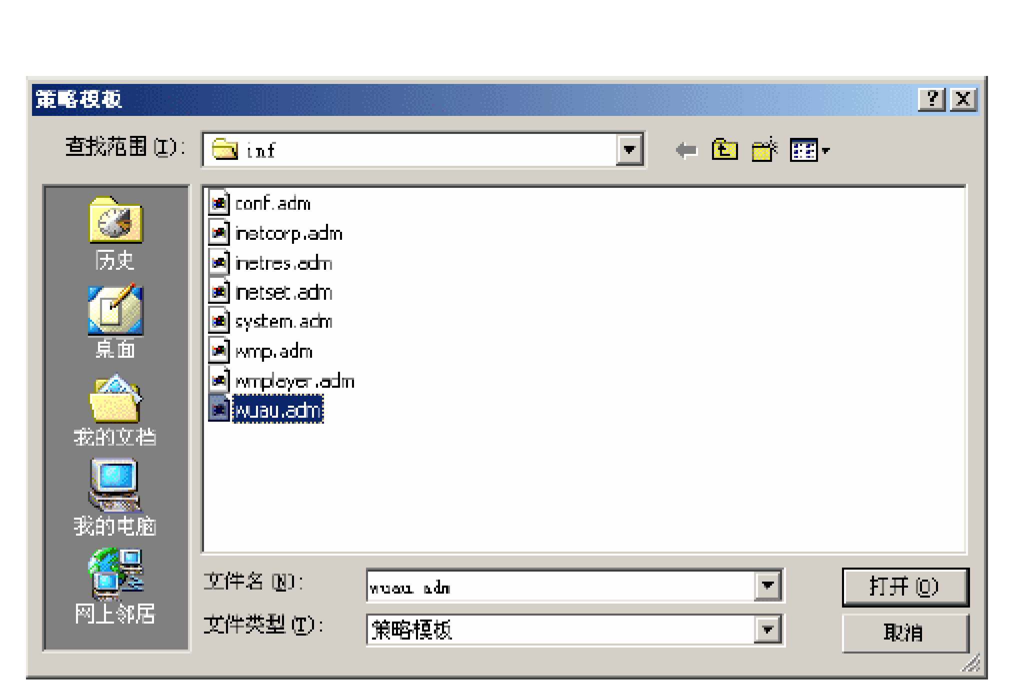



图 6-37 选择策略模板

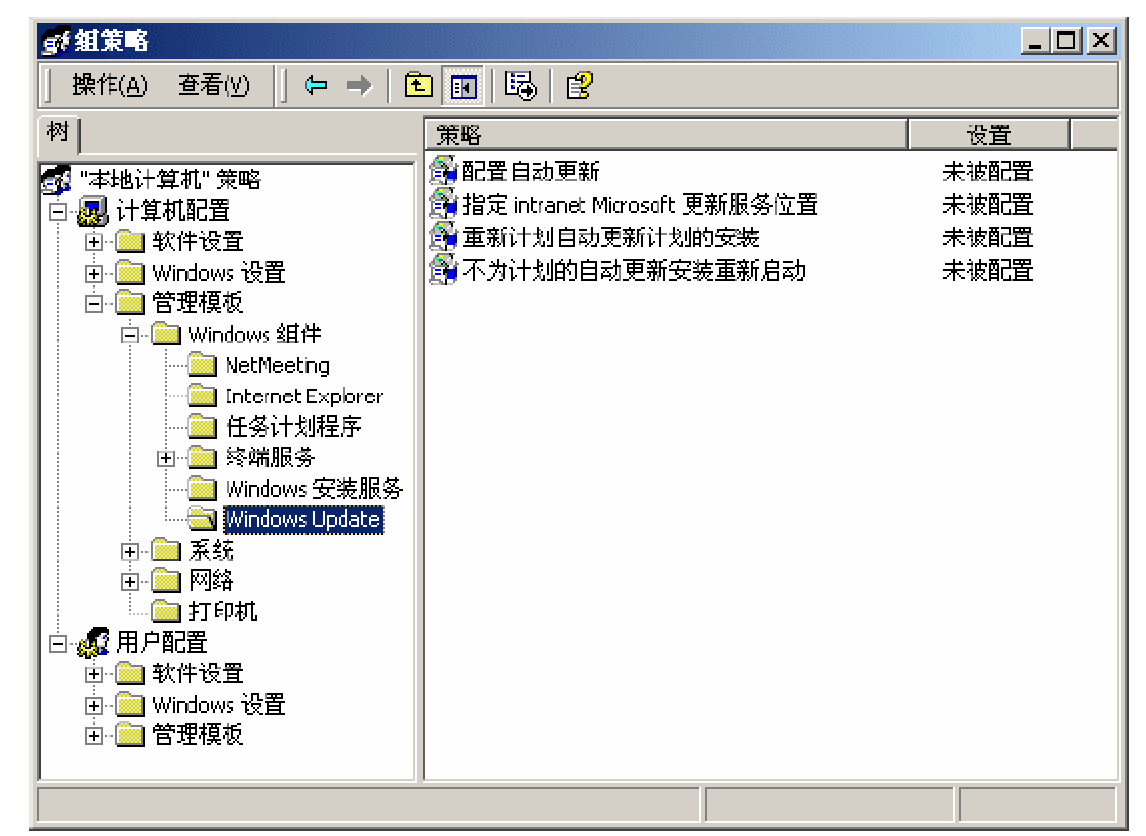


图 6-38 Windows Update



说 明

如果系统是 Windows XP、Vista、Windows 7，则直接从第（4）步开始配置。

05 双击“配置自动更新”项目，显示如图 6-39 所示“配置自动更新 属性”对话框。单击“启用”单选按钮，在“配置自动更新”列表中选择自动更新的方式，建议选择“3 - 提醒下载并提醒安装”选项。完成后单击“确定”按钮即可。

06 在“Windows Update”窗口中双击“指定 intranet Microsoft 更新服务器位置”，显示“指定 intranet Microsoft 更新服务器位置 属性”对话框。单击“启用”单选按钮，在“设置检测更新的 intranet 更新服务”和“设置 intranet 统计服务器”文本框中，分别输入 WSUS 服务器地址，格式为“http://WSUS 名称或 IP 地址”，如图 6-40 所示。

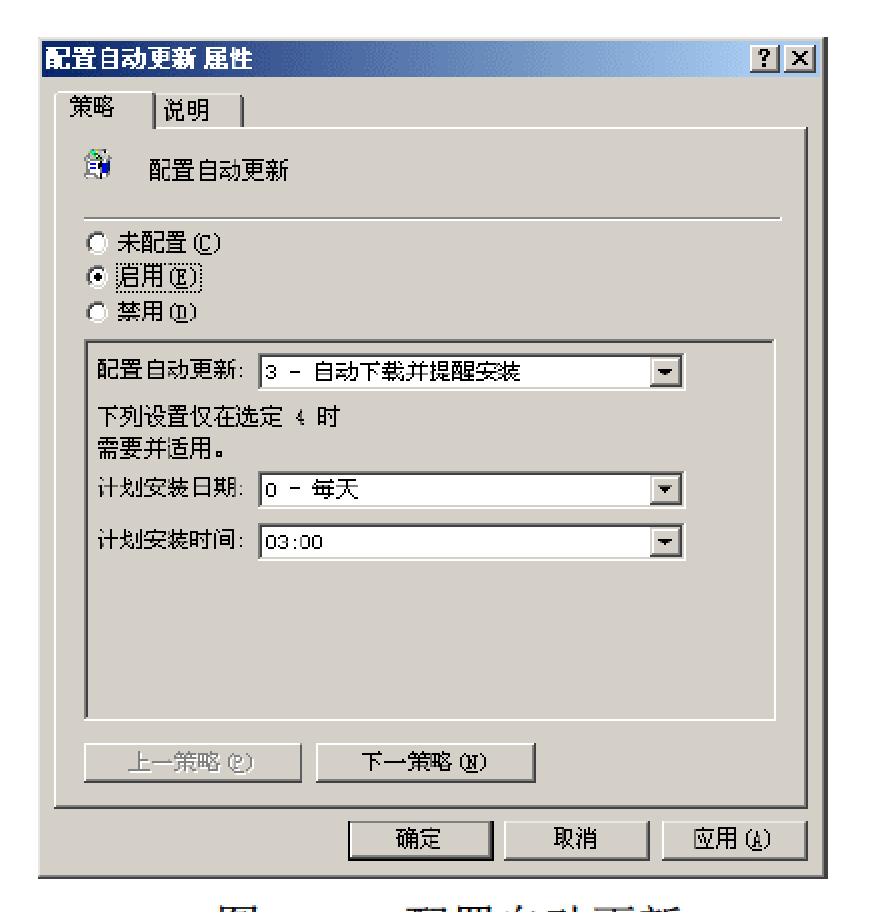


图 6-39　配置自动更新

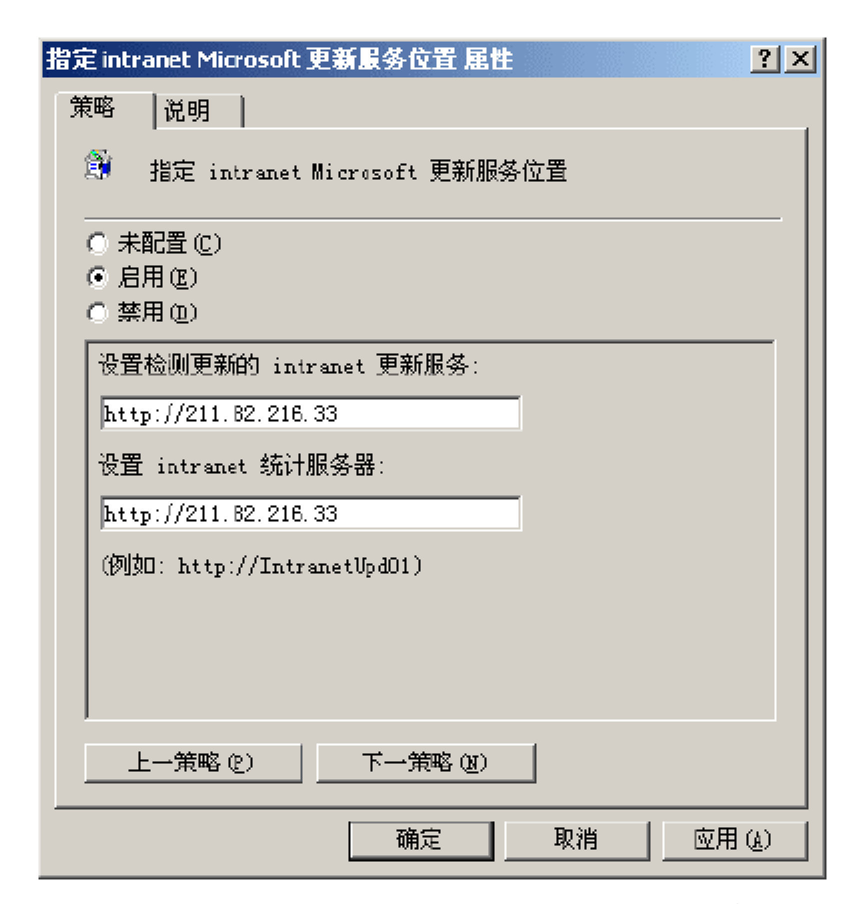
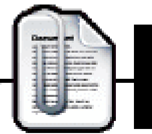


图 6-40　指定 Intranet Microsoft 更新服务器位置



提 示

如果 WSUS 服务器没有使用默认端口，则指定更新服务器和统计服务器时，也需要指定匹配的通信端口，如 http://211.82.216.33:8530。

07 单击“确定”按钮保存设置。这样，Windows 2000、XP、Vista 等操作系统的计算机即可自动从 WSUS 服务器获取更新了。

6.3.2　通过组策略配置客户端

如果网络中的计算机都已经加入到域，则可以在域控制器上，修改组策略中“计算机配置→管理模板→Windows 组件→Windows Update”策略，指定 WSUS 服务器的地址以及其他的选项，其设置方法、步骤与上一节内容相同，不做过多介绍。

修改策略后，在域控制器上，进入命令提示符，执行 gpupdate /force 强制策略更新。

6.3.3　通过导入注册表文件指定 WSUS 服务器

如果网络中的计算机没有加入到域，或者网络中的计算机是一些安装 Windows XP home 操作系统的计算机，则可以通过导入“注册表”的方式，指定 WSUS 服务器。可以在一台计算机上，指定当前网络中 WSUS 服务器的地址以及其他配置参数，然后运行 regedit，将 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate 键值导出注册表文件，然后将此文件通过内部网站、邮件或其他方式发给需要的计算机，双击导入注册表文件即可，下面是一个导出的注册表文件的内容：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
"RescheduleWaitTime"=dword:00000004
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
```

```
"UseWUServer"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"="http://172.30.5.6:8530/"
"WUStatusServer"="http://172.30.5.6:8530/"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\{4B5496D0-0AEE-4C56-834A-15B8D28DAD18}Machine\Software\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"="http://172.30.5.6:8530/"
"WUStatusServer"=http://172.30.5.6:8530/
```

在本例中，WSUS 服务器的地址是 172.30.5.6,服务端口是 8530，那只要修改、替换其中的地址、端口为自己网络中的 WSUS 服务器的地址与端口，并用“记事本”保存成扩展名为 reg 的文件即可使用。

6.3.4 客户端获取并安装更新文件

服务器端批准指定的更新程序后，客户端就可以开始安装了，操作步骤如下。

01 如果是通过域控制器组策略配置的客户端则可以重新登录到域控制器，如果修改的是本地计算机策略，则可以使用强制刷新的方法使其立即生效。

02 正确连接到 WSUS 服务器后，工作站会自动连接 WSUS 服务器并从 WSUS 服务器下载补丁，当补丁下载完成后，会在右下角出现黄色的“”并提示“已经为您的计算机准备好更新，单击此处安装这些更新”，如图 6-41 所示。

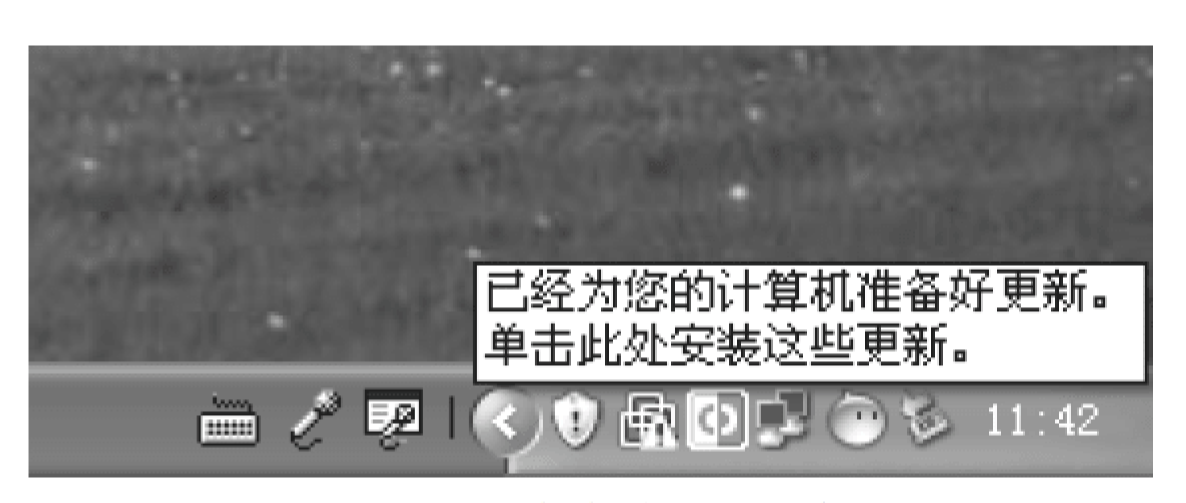


图 6-41 客户端提示信息

03 单击信息提示框开始安装所需更新，显示如图 6-42 所示的选择安装方式提示框，当然是否出现该提示框和前面修改本地策略或域控制器组策略时选择的方式是一致的，如果默认下载并安装则不会出现提示框而是直接安装更新了。这里提供了两种安装方式，快速安装和自定义安装，建议选择快速安装。

04 单击“安装”按钮即可开始安装，显示如图 6-43 所示的“正在安装更新”窗口，此时用户可以最小化当前窗口继续其他操作。根据需要安装的更新内容的多少，需要的时间也会有所不同，安装完成后同样会在系统任务栏出现气泡提示框。

05 安装完成后有些更新内容必须重新启动计算机后才可以生效，所以可能会提示重新启动计算机。



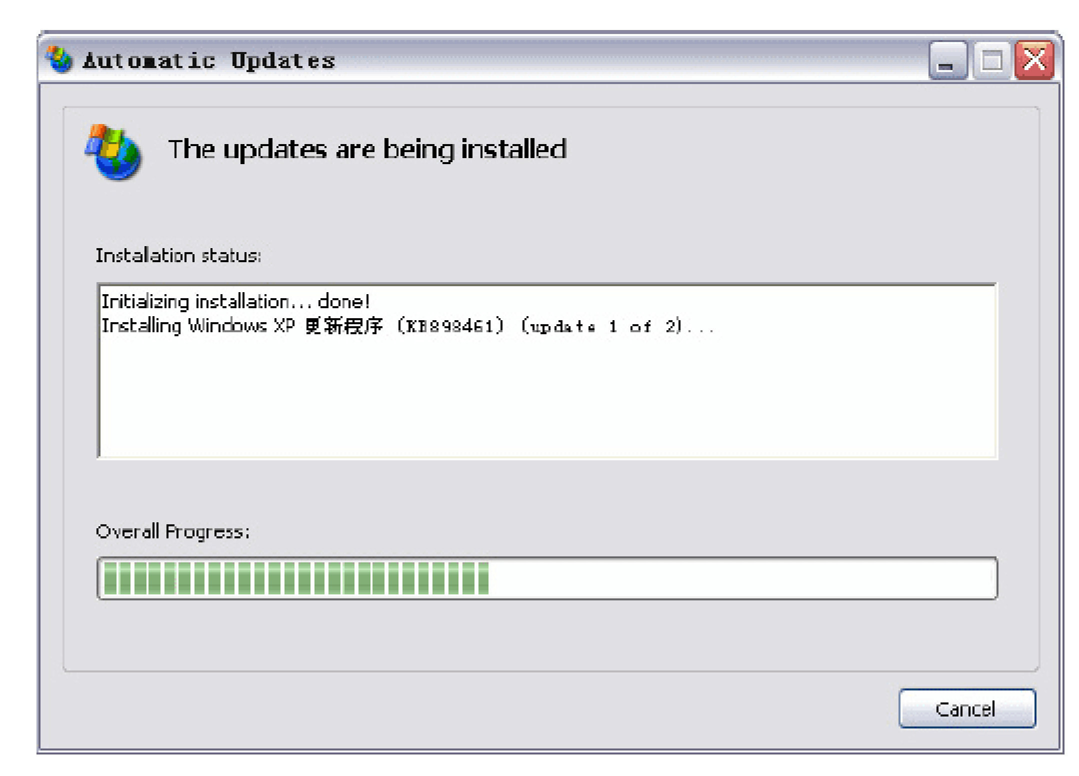



图 6-42　选择安装方式　　　图 6-43　正在安装更新

6.4　WSUS 常见故障解决

WSUS 服务器在网络中的重要性毋庸置疑，但 WSUS 服务器的使用也不是一帆风顺的，本文将介绍使用 WSUS 服务器中，碰到的几个重要问题并介绍解决方法，以方便用户的使用。

6.4.1　关于 CPU 占用率 100%问题

当用户第一次配置 WSUS 服务器，为网络中的计算机提供升级服务时，刚开始为工作站配置使用 WSUS 服务器升级时，有些工作站的速度会非常慢。这时，在这些工作站的“任务管理器”中，会显示 CPU 占用率 100%，而在“进程”选项卡中查看时，将会发现 svchost.exe 进程占用了 100%或者占用了将近 100%的 CPU 资源，如图 6-44、图 6-45 所示。

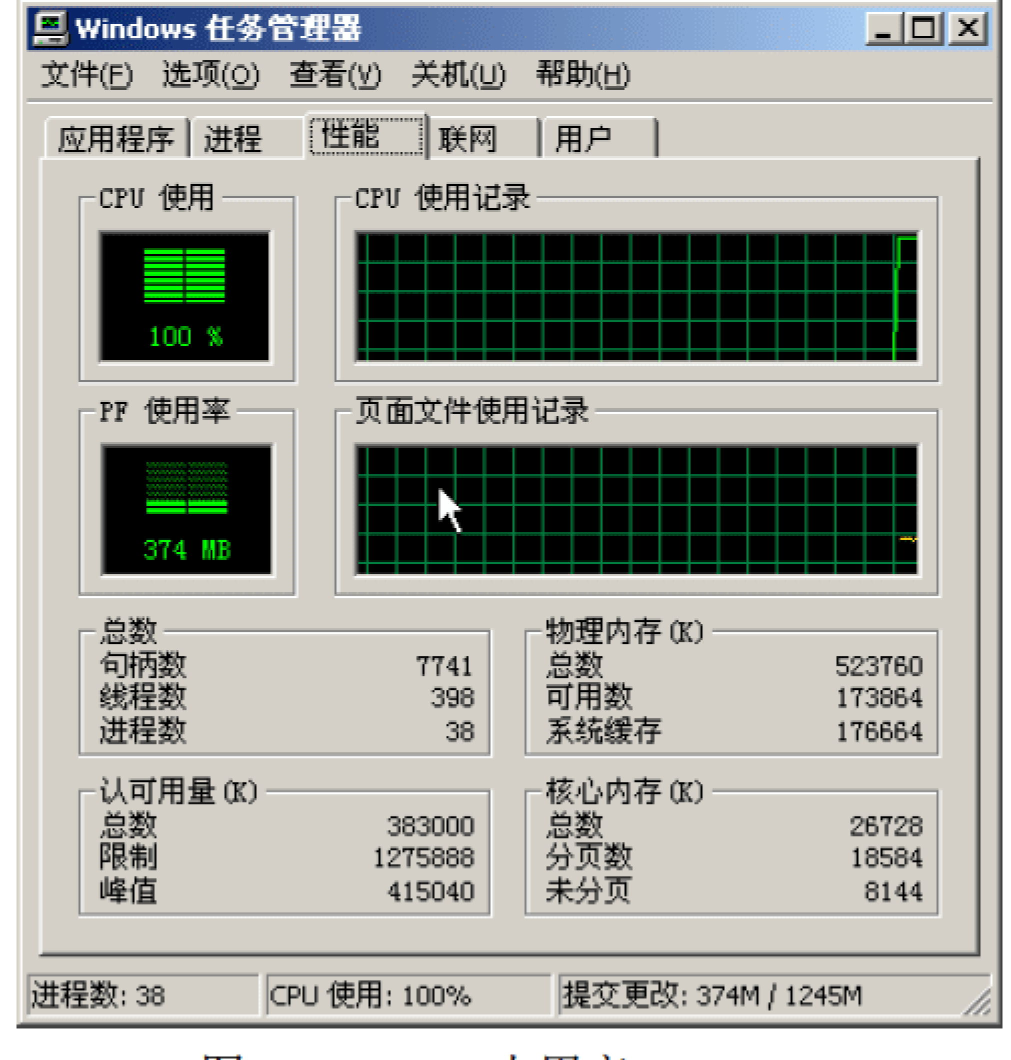


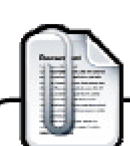
图 6-44　CPU 占用率 100%



图 6-45　svchost.exe 占用了大量 CPU 资源

当工作站出现这个问题时，可以暂时中止 svchost.exe 进程，然后从“http://download.

microsoft.com/download/7/6/6/766c2a2c-dc75-4417-8afe-7ed5c4ec1b06/WindowsXP-KB927891-v3-x86-CHS.exe”下载补丁，在工作站上安装这个补丁，重新启动计算机，就可以解决该问题。需要注意，在安装补丁的时候，只有出现图 6-46、图 6-47 的界面，才表示补丁正确安装。在有的工作站上，需要反复多次安装这个补丁，才能解决问题。



说 明

WSUS 服务器也已经提供这个补丁，但由于各种原因，有的工作站不能及时安装这个补丁，就会出现 CPU 占用率 100%的现象。

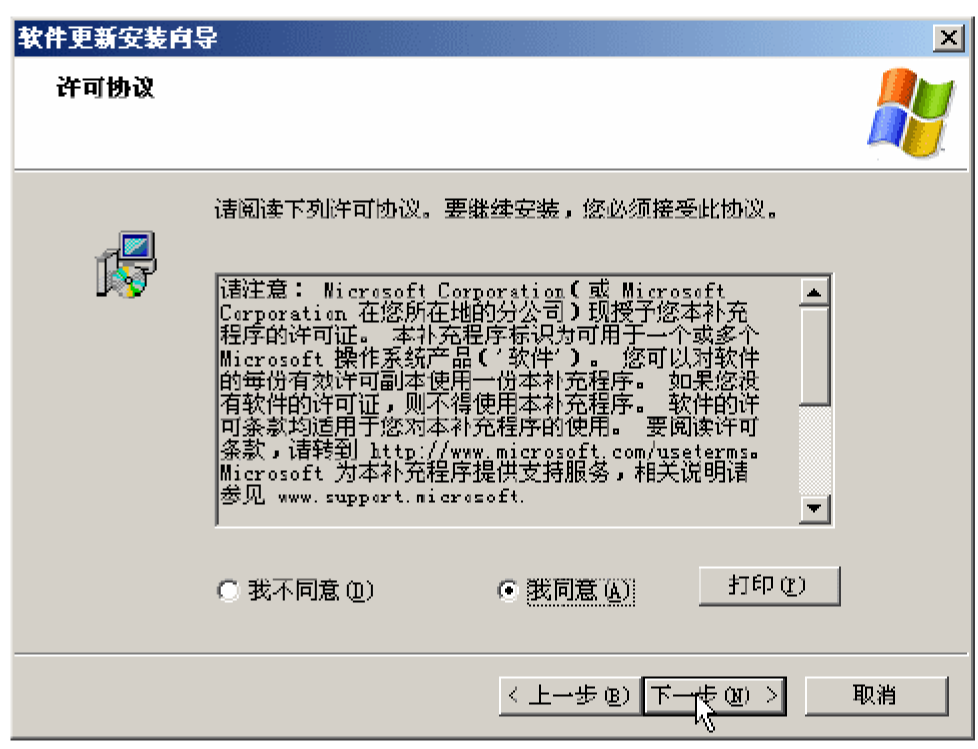
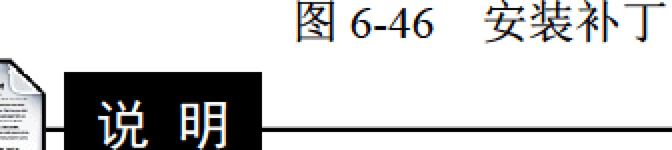




图 6-46　安装补丁

图 6-47　安装 KB927891 补丁完成



说 明

当 WSUS 在后台自动安装补丁时，CPU 占用率暂时会达到 100%，但不会一直达到 100%，而是在 40%～100%之间反复，出现这种情况是正常的。

6.4.2　工作站不能连接上 WSUS 服务器的问题

当使用 gpedit.msc 配置工作站以使用 WSUS 服务器更新时，或者使用编辑好的“注册表文件”导入工作站，以从企业内部的 WSUS 服务器升级时，第一次使用时，为了让工作站立刻从 WSUS 服务器下载补丁，在命令提示符下使用：

```
wuauclt /detectnow
wuauclt1 /detectnow
```

之后，再使用 netstat –an 时，没有发现到 WSUS 服务器的连接。

或者，没有使用上述命令（此时工作站会在管理员规定的时间从 WSUS 服务器下载并安装补丁），但在经过几天之后，工作站没有从 WSUS 服务器下载任何补丁，并且在 WSUS 服务器上，也没有发现该工作站（可以通过计算机名称、IP 地址检查），此时需要在该工作站上安装“WSUS 客户端代理”程序，并重新启动计算机，将解决这个问题。程序下载地址为：

http://download.windowsupdate.com/WindowsUpdate/redist/standalone/7.0.6000.381/WindowsUpdateAgent30-x86.exe

安装提示如图 6-48、图 6-49 所示。

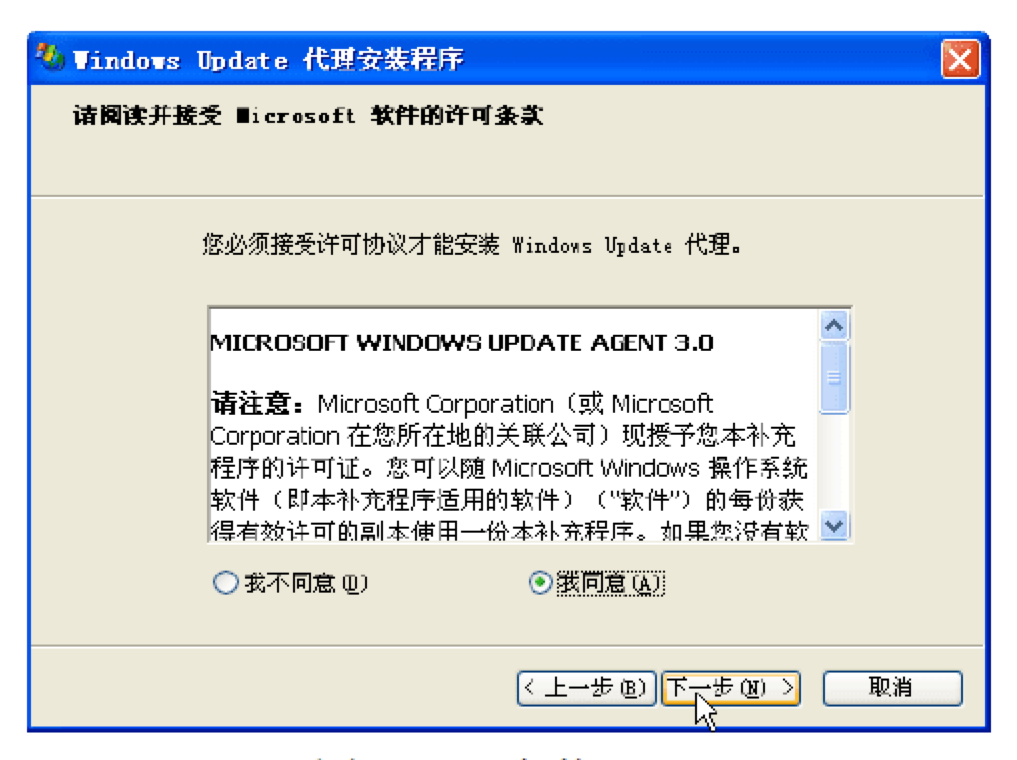



图 6-48 安装 update agent

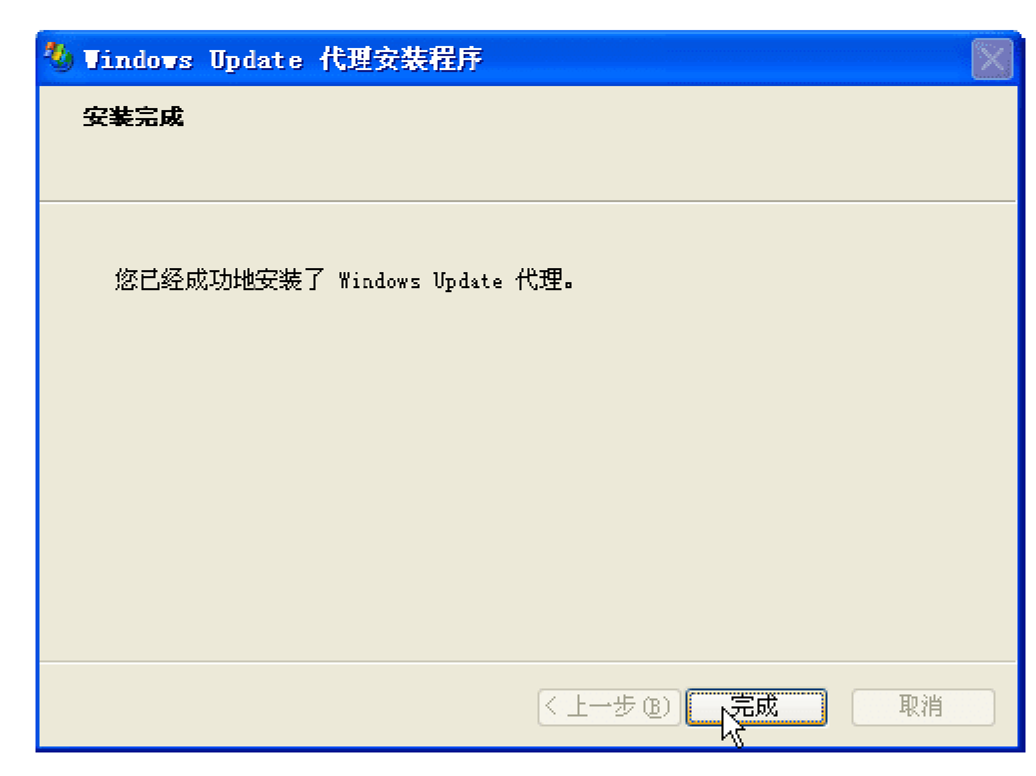


图 6-49 安装完成

6.4.3 关于自动更新的问题

当工作站端配置为“自动下载并计划安装”时，工作站将会在指定的时间安装，配置界面如图 6-50 所示。可能有的朋友认为，这样工作站不会在指定的时间安装，但经过多次测试，结果如下。

当工作站从 WSUS 服务器下载完补丁后，会在右下角出现黄色的“ ”图标并提示“已经为您的计算机准备好更新，单击此处安装这些更新。”，如图 6-51 所示。

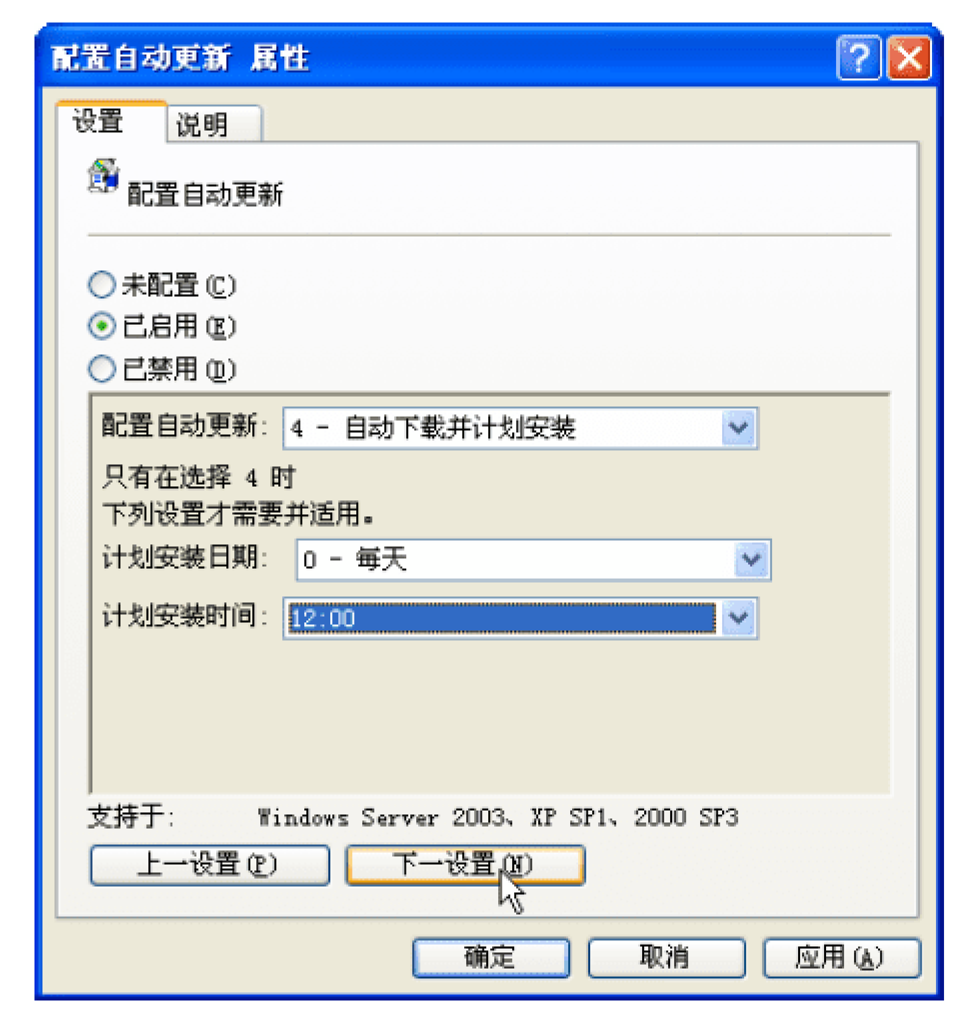


图 6-50 设置自动更新属性

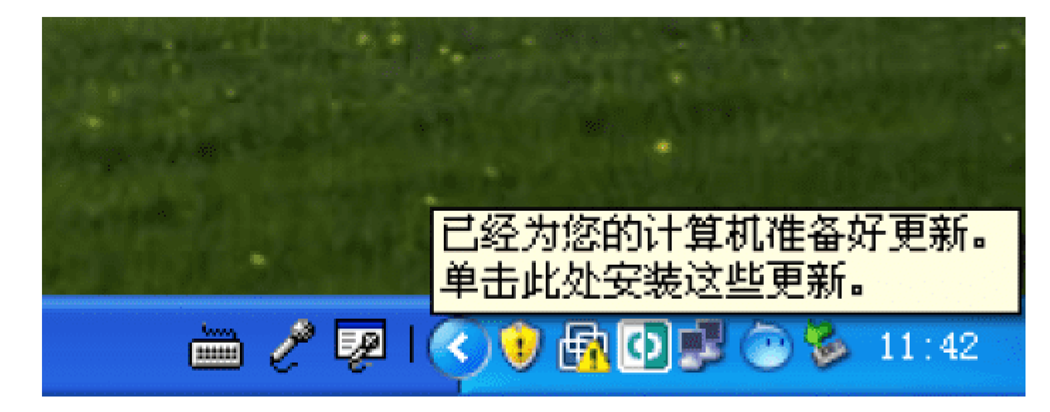


图 6-51 提示补丁已经下载完成

根据用户是否选择，将会有三种情况：

（1）如果用户单击“ ”图标，会弹出如图 6-52 所示的对话框，此时单击“安装”按钮，即可开始安装补丁。

（2）如果用户没有选择，则在到达图 6-50 所设置的时间后，WSUS 客户端程序会自动在后台安装补丁，这时，如果打开“Windows 任务管理器”，在“进程”选项卡中，会发现一个 svchost.exe 进程占用了大量的 CPU 资源，并且占用了大量内存，这个进程会完成补丁的自动安装工作，如图 6-53 所示。另外，还可以在“进程”选项卡中看到安装的补丁，如图 6-54 所示。



图 6-52　手动安装补丁



图 6-53　WSUS 在后台安装补丁



图 6-54　在后台安装的补丁

安装完成后，安装的补丁需要重新启动计算机，如果 WSUS 客户端将“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”这一项设置为“禁用”或“未配置”（如图 6-55 所示），则会弹出 5 分钟倒计时窗口，并在达到指定时间内，如果无人取消该操作，计算机将会重新启动。如果配置为“已启用”，则会弹出“更新完成，是否需要重新启动计算机”的提示。如果安装的补丁不需要重新启动计算机，则不会有任何提示。

（3）如果在指定的时间没有安装，则 Windows XP 会在“关机”的时候，安装该更新，如图 6-56 所示。

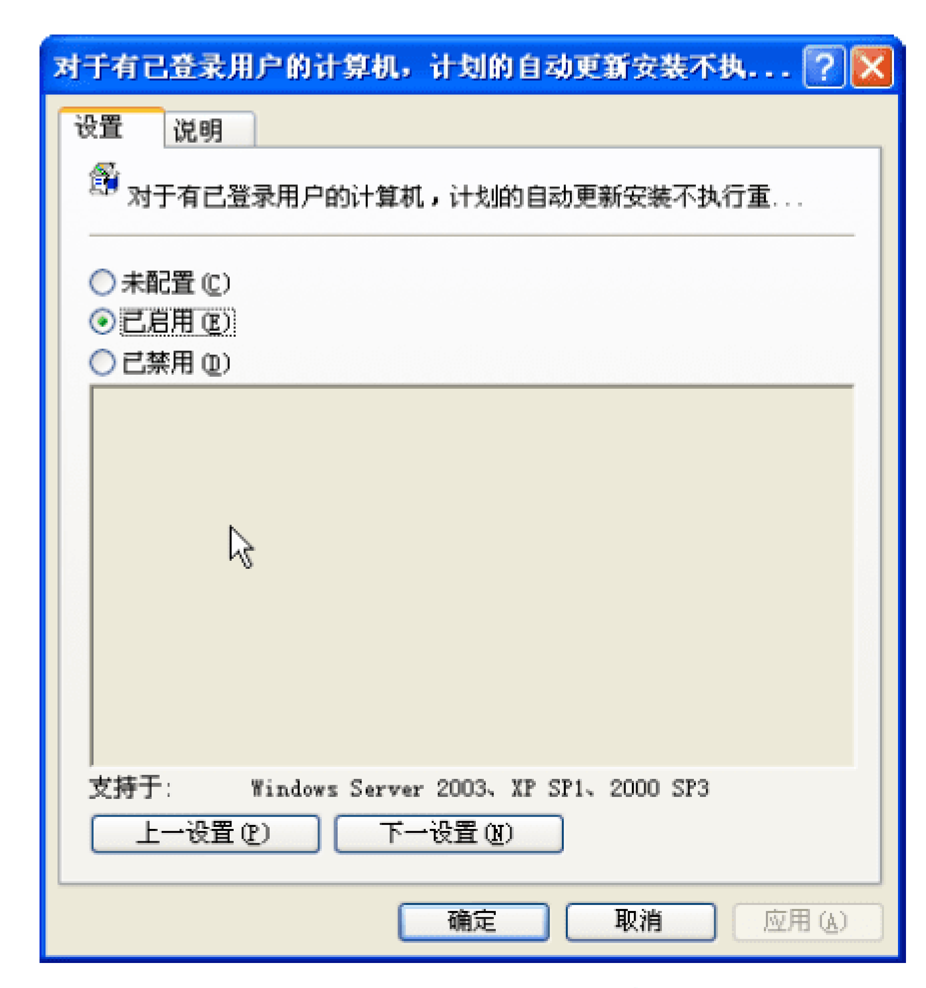


图 6-55　配置自动启动



图 6-56　自动安装更新

6.4.4　服务器使用 WSUS 的问题

对于 Windows Server 2008、Windows Server 2003 的服务器来说，最好设置服务器在夜间自动安装并自动重启，设置关键点为：

- 在图 6-50 中，选择服务器空闲时间，例如晚上 11:00 之后，上午 5:00 之前。
- 在图 6-55 中，单击“未配置”或“已禁用”单选按钮。

6.4.5　关于 Vista/Windows 7 客户端的问题

当工作站是 Vista 或 Windows 7 操作系统时，除了可以使用 wuauclt 命令立刻从 WSUS 服务器检查并下载补丁，还可以在“控制面板→Windows Update”中，单击“检查更新”（如图 6-57 所示），立刻从 WSUS 服务器检查并下载更新补丁；如果不使用 WSUS 服务器，可以单击“在线检查来自 Microsoft Update 的更新”从 Microsoft 网站检查升级补丁。

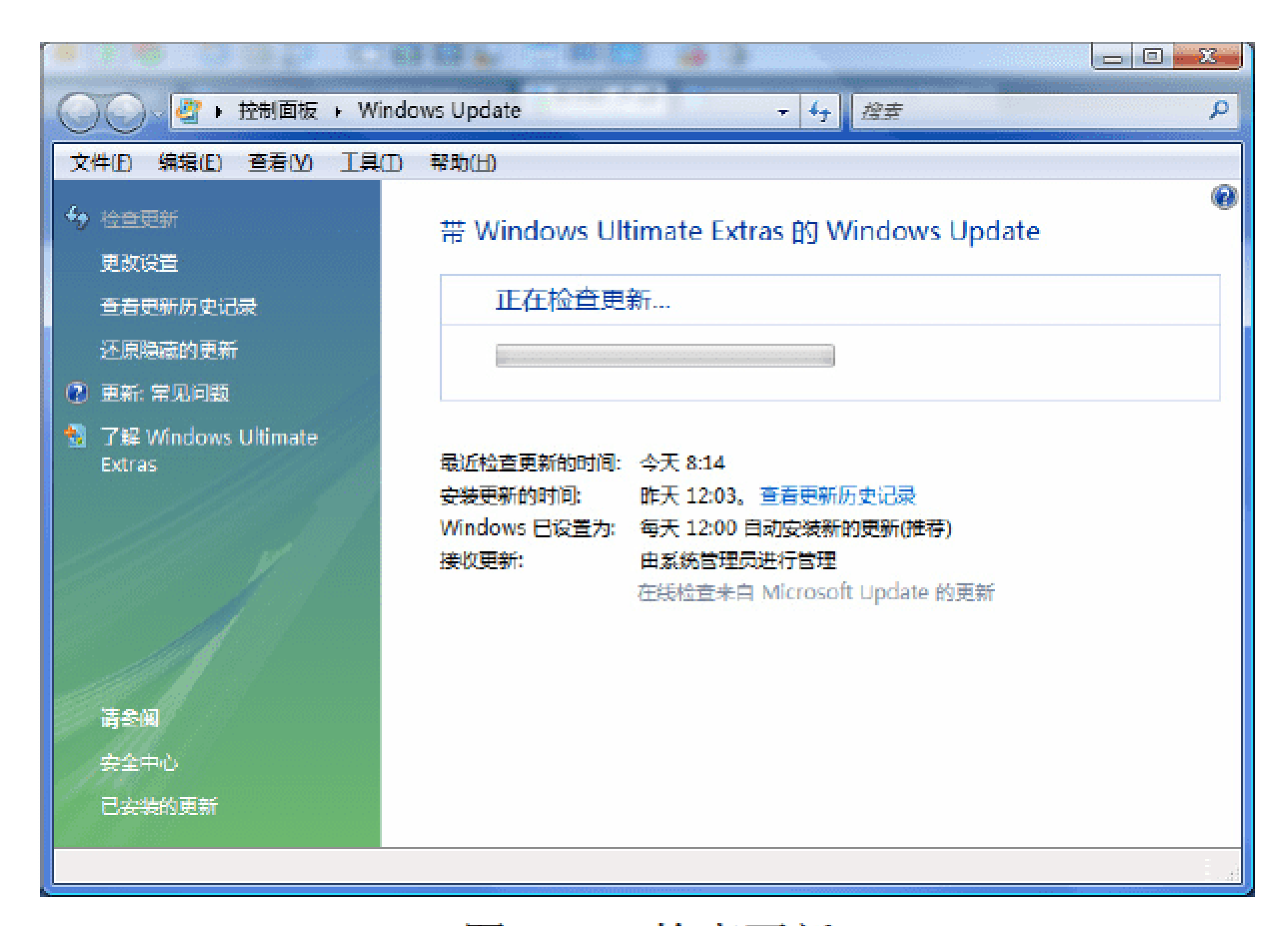


图 6-57　检查更新

6.4.6　关于 Windows XP SP3 补丁的问题

在 WSUS 服务器上，Windows XP SP3 补丁不能自动审批，需要管理员在 WSUS 服务器上，手动审批该补丁，如图 6-58 所示。

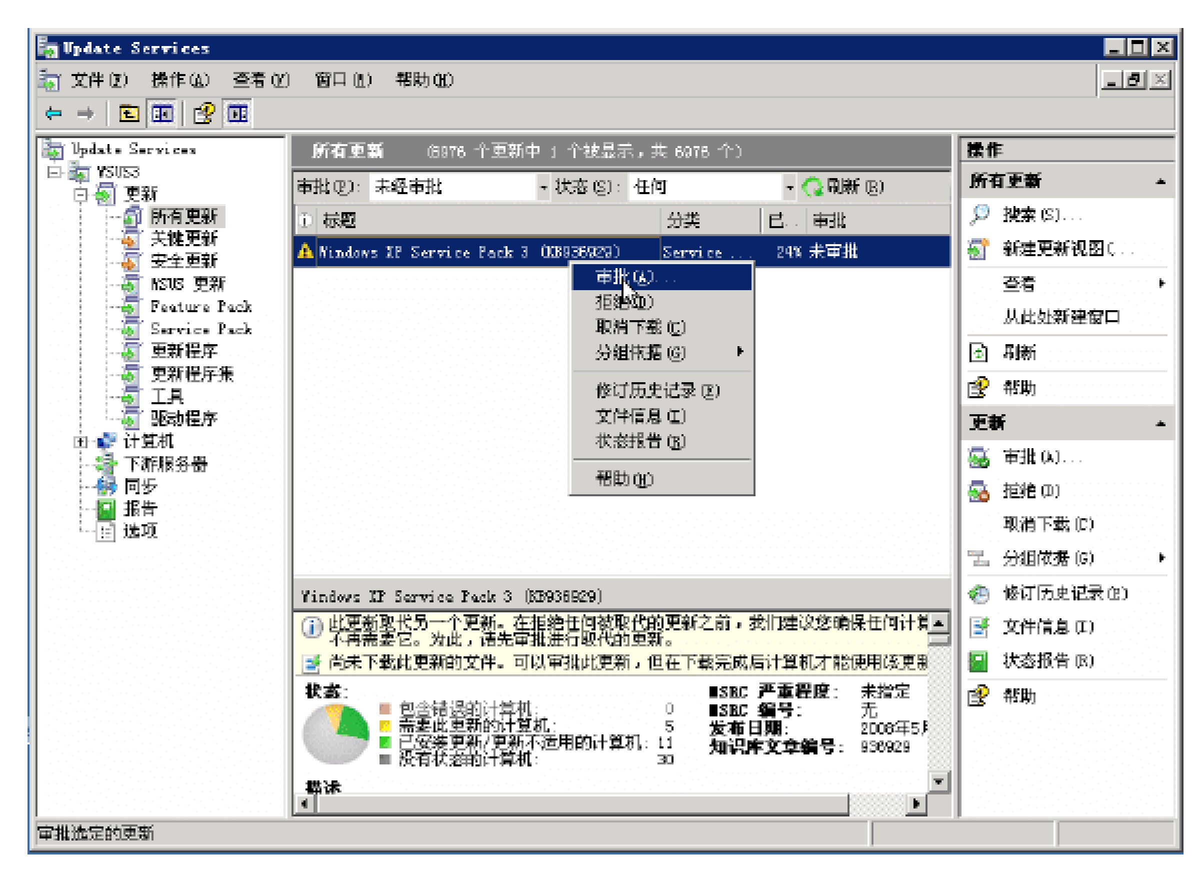


图 6-58　Windows XP SP3 更新需要手动审批

6.4.7　升级到 XP SP3 后出现“0x80070002”错误

在审批 XP SP3 后，网络中的一些工作站出现 “一个问题阻止 Windows 正确检查此机器的许可证。错误代码 0x80070002”的提示，然后注销计算机，当再次进入后，仍然提示此错误，不能正常使用。

这是由该计算机安装的是“破解”版本的 Windows XP 操作系统造成的。一般情况下，使用 WSUS 服务器，为网络中的工作站提供升级补丁时，不会检测操作系统是否正版，但在以下的情况下例外：

- 安装 Windows Media Player 11 的时候。
- 安装 IE 7.0 的时候（后来取消了这个限制）。
- 升级到 XP SP3 时。

出现这个问题后，虽然一些资料上说，恢复 C:\windows\system32 下的 oembios.bin 文件即可，但实际上，这个问题大多数情况下均需要重新安装操作系统才能解决。在重新安装的时候，建议使用 Windows XP 的 VL 版本，而不要使用“破解”版或某些“精简”版。

6.4.8　WSUS 服务器出现“此服务器不支持必要的 HTTP 协议”错误

当 WSUS 服务器不能下载某些补丁，并且在“事件查看器”中可以看到“内容文件下载失败。原因：此服务器不支持必要的 HTTP 协议。后台智能传送服务（BITS）要求服务器支持范围协议头”的描述，如图 6-59 所示。

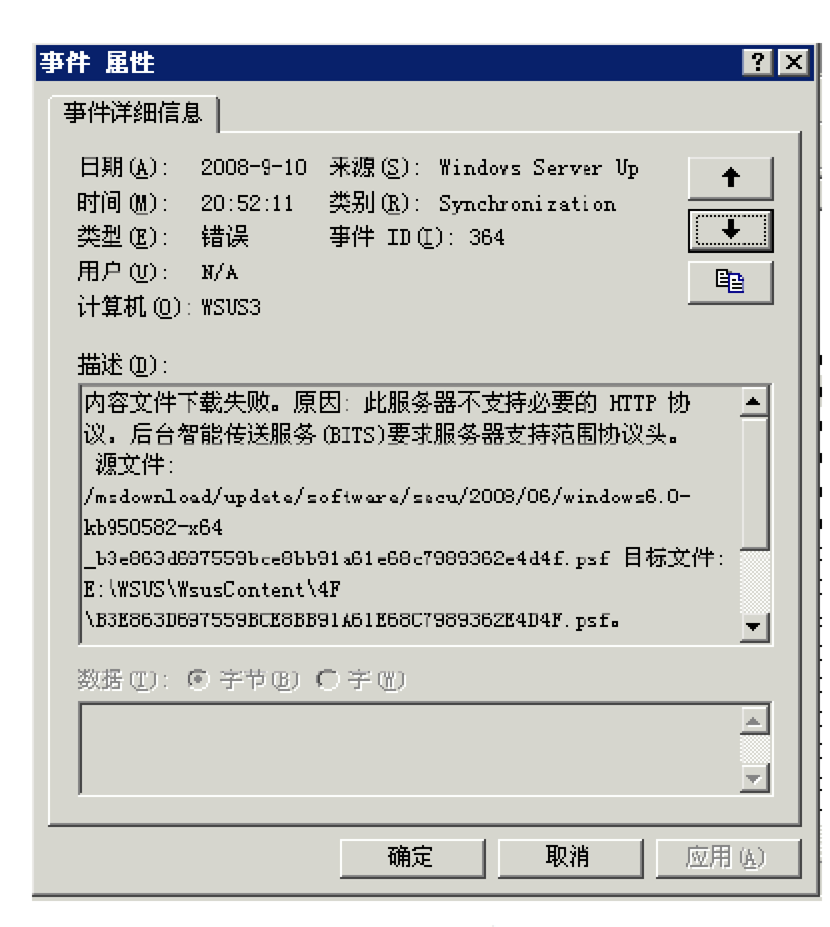


图 6-59　WSUS 服务器不能下载

经过分析，可能是单位防火墙的设置问题，可以暂时把 WSUS 的 BITS 服务关闭，就能解决这个问题。在 WSUS 中不使用 BITS 下载而是直接下载补丁的方法如下：

01 首先从“http://download.microsoft.com/download/

7/7/4/7745a34e-f563-443b-b4f8-3a289e995255/WSUS%20Server%20Debug%20Tool.EXE”下载 WSUS Debug 工具。这是一个自解压的程序，下载之后，运行这个程序，将该程序解压到一个文件夹中，例如 C 盘的 1 文件夹中，如图 6-60 所示。

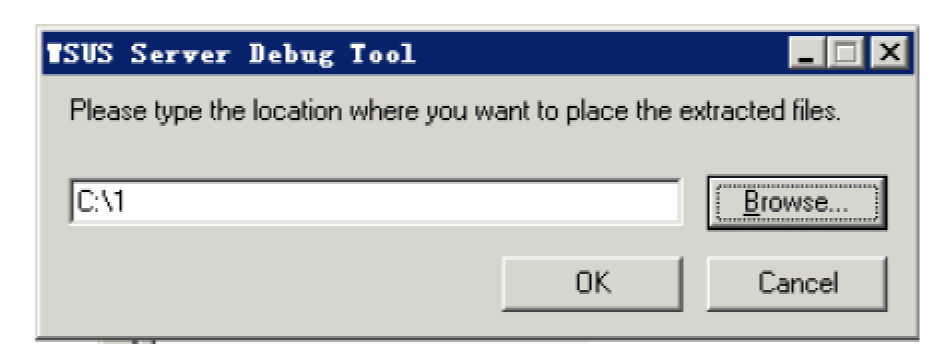


图 6-60　指定解压缩路径

02 在 Windows Server 2003 安装光盘中，从“support\tools”文件夹中找到 sup_srv.cab 文件，从该文件中解压缩 bitsadmin.exe 程序到图 6-60 中的路径。

03 进入命令提示符，进入图 6-60 解压缩的路径，执行 wsusdebugtool /tool:setforegrounddownload 命令，禁止使用 BITS 下载更新，而是直接下载更新，如图 6-61 所示。

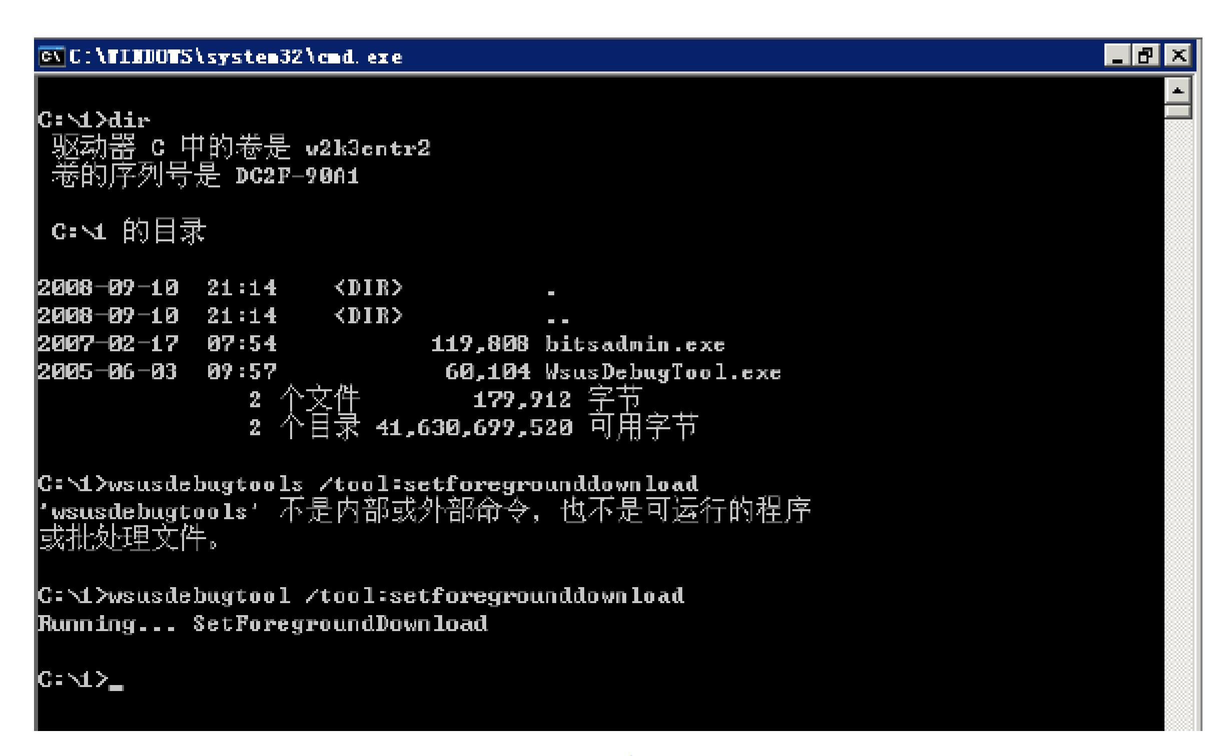


图 6-61　直接下载更新

04 再次进入 WSUS，同步 WSUS（如图 6-62 所示），返回到“事件查看器”中，不会再出现类似图 6-59 的错误提示。

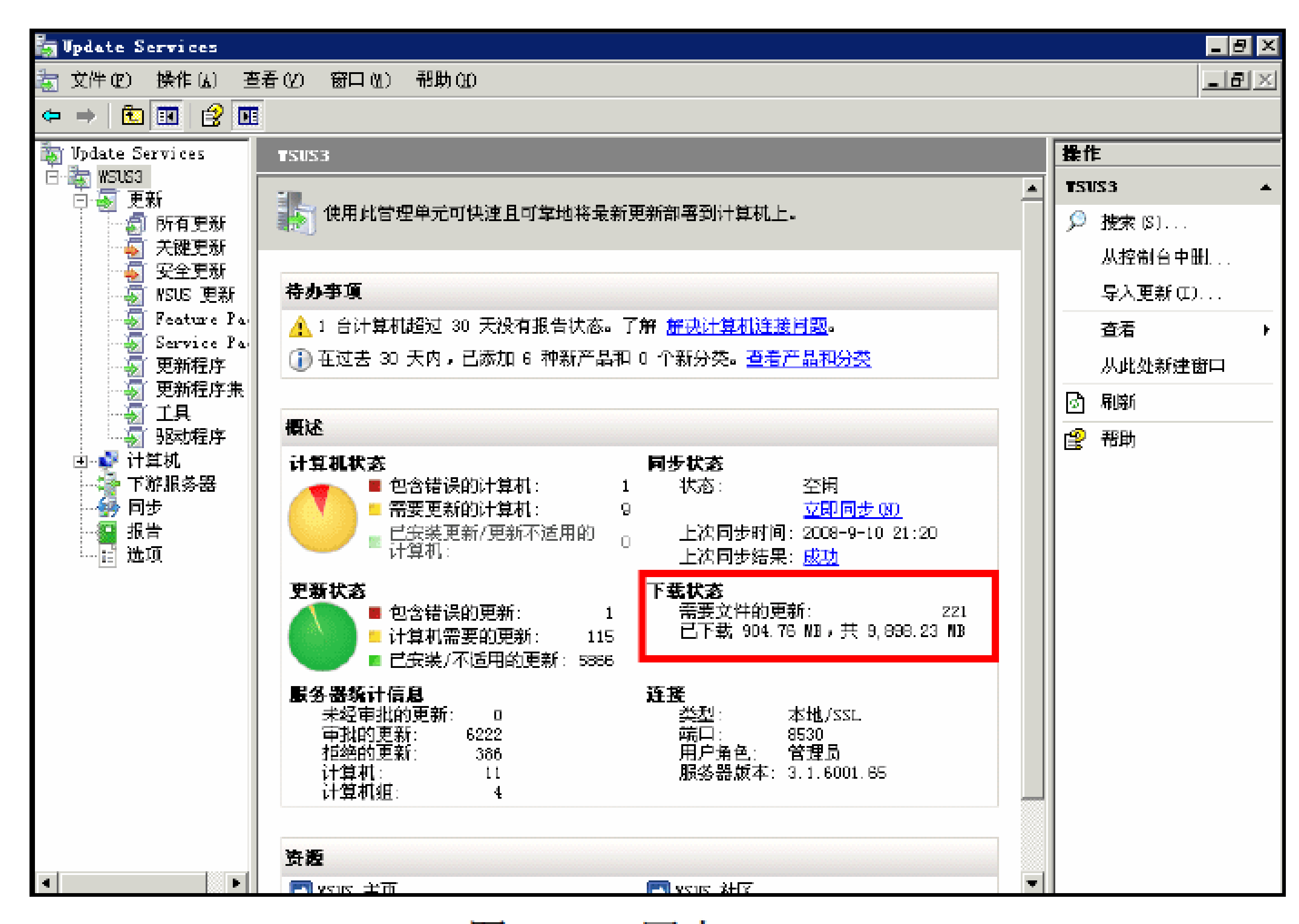


图 6-62　同步 WSUS

在图 6-62 中，从 21:20 开始同步，不到 20 分钟的时间，已经下载了 900MB 左右的补丁。

隔一夜之后，可能仍然会出现“WSUS 不能下载”的错误，但 WSUS 已经下载了大量的、以前不能下载的补丁，进入命令提示符，重新运行 wsusdebugtools.exe /tool:setforegrounddownload，然后再同步 WSUS，继续下载，多下载几次也就可以了。这样，虽然每次都能出现错误，但每次都能下载补丁，直到把所有的补丁下载完。

同时，还可以在“选项”对话框中，把 WSUS 从上游服务器的同步次数增加，以解决“WSUS 不能下载”的错误。

第 2 篇

Active Directory网络管理与应用



第 7 章 Active Directory 网络管理

Windows Server 2008 R2 是 Microsoft 公司最新的服务器操作系统，安全性高，配置灵活、方便，集成了 Hyper-V 虚拟化功能，能够充分发挥硬件的性能。Windows Server 2008 R2 改写了底层的网络传输代码，理论上，在传送大文件时，速度要比 Windows Server 2003 快 8 倍以上。由于 Windows Server 2003 已经不能充分发挥硬件的性能，因此，在未来的几年中，原来基于 Windows Server 2003 的服务器平台都将逐步升级到 Windows Server 2008 及 Windows Server 2008 R2。

7.1 Windows 网络应用概述

在现代企业网络中，为了提高网络的安全性，减轻网管与最终用户的负担，需要在网络中部署多种服务器。例如，用于企业内网、外网隔离的防火墙与代理服务器、用于内网 TCP/IP 地址分配的 DHCP 服务器、用于名称解析的 DNS 服务器、用于 NetBIOS 名称解析的 WINS 服务器、用于操作系统远程安装的 RIS 与 Windows 部署服务器、用于操作系统与应用软件补丁的 WSUS 服务器、用于邮箱的邮件服务器、用于企业即时消息与视频会议的 OCS 2007 服务器、用于 Windows 服务器与工作站管理的 SCOM 2007 服务器、用于企业安全的证书服务器等。这些服务器综合应用、互相配合，可以让企业网络处在可管理的、安全的状态下。同时，连接这些服务器与工作站的交换机、路由器等也是必不可少的。如图 7-1 所示是一个基于 Windows 网络的，包括各种服务器并且用来提供各种服务的网络拓扑图。

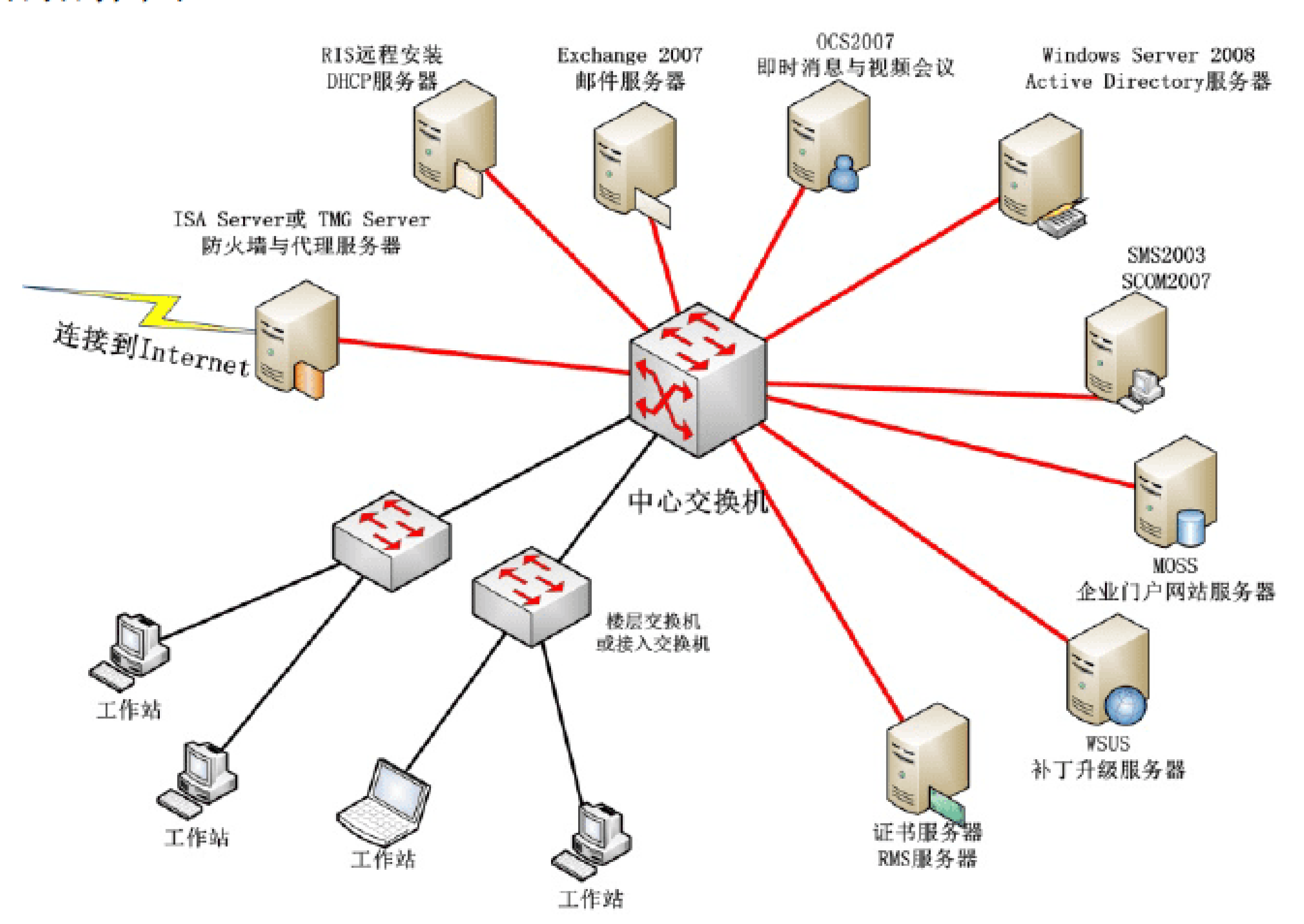


图 7-1 Windows 网络拓扑图

7.1.1 Windows 服务器规划

Windows 产品比较多，并且每个产品的功能、用途也不同。在实际的网络中，很少有企业需要部署所有的 Windows 产品，通常都是根据自己企业的特点和实际需求，部署其中的若干种服务器。下面将介绍各种 Windows 服务器的名称、用途，及其相关关系，以便用户根据自己企业的情况加以选择。

1. Active Directory 服务器

Active Directory 的中文名称为“活动目录”，简称为 AD。活动目录服务器是 Microsoft 其他服务器的基础，负责对网络中的所有工作站及所有服务器进行“集中”管理，例如 Exchange 服务器、DFS 与文件服务器、RIS 与 Windows 部署服务器等。

从 Windows 2000 开始，Microsoft 引进了“组织单位（OU）”等概念，并设计了 Active Directory 网络方式，相对于以前的 Windows NT 域，Active Directory 增加了更多的功能。以前的 NT 网络，基本上处于“人工”状态，如果网络中的工作站需要进行安装程序、系统升级或安装操作系统等工作，都需要管理员到每一台工作站上直接操作。当工作站的数量非常多时（如 500 台或 1000 台以上），工作量将非常大，而使用 Active Directory 服务就很容易解决这个问题。Active Directory 服务可以实现以下几点：

- 应用程序能“自动”通过网络进行安装。
- 用户的文档、程序以及设置（比如 Office 程序的设置、桌面的图标、其他应用程序的参数设置）自动保存在网络中的文件服务器上，并自动与本地的工作站进行同步。如果需要，员工可以在指定的计算机上使用属于自己的用户名和密码登录，而文档与设置也随员工“跟随”到每一台计算机，并且每名员工只能使用他们自己的文档，不能查看其他的文档与数据，反之亦然。
- 由于员工的数据已经提前备份到了网络中的服务器上，当员工的计算机硬盘或者计算机损坏时，不需要网络管理员恢复数据。只要让员工更换损坏的部件，重新安装系统，并使用自己的用户名、密码登录，数据即可自动从服务器还原。
- 如果员工忘记了自己的登录密码，不需要找“网络总管理员”，只要找其部门中的一个技术人员，就可以修改自己部门员工的登录密码。

可见，只要实现了上述网络环境和系统配置后，用户就能够完成从操作系统的安装、软件部署，到用户定制、用户数据备份等步骤的全自动操作。

2. Windows Server 2008

使用 Windows Server 2008 及 Windows Server 2008 R2，IT 专业人员对其服务器和网络基础结构的控制能力更强，从而可重点关注关键业务需求。Windows Server 2008 R2 通过加强操作系统和保护网络环境提高了安全性，可以加快 IT 系统的部署与维护，使服务器和应用程序的合并与虚拟化更加简单，提供直观管理工具，操作更灵活。

3. DHCP

DHCP 服务器可以自动为网络中的“所有工作站”分配 TCP/IP 地址、子网掩码、网关地址、DNS 服务器地址及 WINS 服务器地址，从而大大减轻网络管理员的负担，并且避免由于 TCP/IP 地址设置等问题引起网络故障。

4. DNS

DNS 服务器为“所有工作站”互相访问（使用 DNS 名称访问）、“所有工作站”与“所有服务器”互相访问、以及“所有工作站”和“所有计算机”访问 Internet 提供名称解析服务，负责把类似于“www.sohu.com”、“server.heinfo.local”解析成对应的 TCP/IP 地址。

5. WINS

WINS 服务器为“所有工作站”、“所有服务器”之间使用“NetBIOS 名称”互相访问提供解析服务，负责把类似于“computer”的计算机名称解析成对应的 TCP/IP 地址。

6. RIS 远程安装服务器

RIS 服务器是 Windows 2000 Server、Windows Server 2003 内置的服务，可以为没有安装操作系统的“所有工作站”远程安装 Windows XP、Windows 2000、Windows Server 2003 操作系统。

7. Windows 部署服务

Windows 部署是 RIS 服务的升级版本，它集成在 Windows Server 2008 中，可以为网络中的计算机远程部署 Windows Vista 与 Windows Server 2008 操作系统。

8. WSUS 服务器

WSUS 用于为 Windows 2000、Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008 操作系统提供补丁服务，同时也为 Microsoft 系列软件如 Office、SQL Server、ISA Server、Exchange Server 等产品提供补丁服务。

9. Forefront TMG Server

Forefront TMG Server 是 Microsoft 的防火墙与代理服务器软件。在使用 Forefront TMG Server 时，可以让“指定的计算机”在“指定的时间”、以“指定的协议”访问“指定网络”中的“指定的服务器”。Forefront TMG Server 的配置非常灵活，使用简单、方便。

10. 证书服务器

证书服务器用于局域网、广域网的安全通信，可以用于“所有用户”之间发送安全加密的电子邮件、用于“Web 服务器”对外提供安全的 Web 访问、用于“远程工作站”安全访问企业内部局域网。

11. Exchange 邮件服务器

Exchange Server 系列是 Microsoft 的电子邮件服务器，可以为“所有工作站”、“远程工作站”、Internet 用户提供电子邮件服务。Exchange Server 在使用时需要 Active Directory 的支持。

12. 视频会议与即时消息服务器

Microsoft Lync 2010 是带有即时消息、会议和语音功能的真正的统一通信客户端。Lync 2010 通过更新的用户界面将通信工具组合在一起，用户可按照习惯的方式使用它们。此客户端的特点是带有仪表板，用户可以轻松地查找和使用常见功能，比如拨号盘、可视语音邮件、联系人列表和活动对话列表。

13. SCOM 2007 系统管理服务器

SCOM 2007 的全称是 System Center Operations Manager 2007，用于管理 Microsoft 系列服务器与工作站，它也需要 Active Directory 的支持。

14. 其他服务器

在 Windows 网络中，还要用到其他服务器。例如，DFS 服务器可以将网络中的“所有服务器”联合起来，使用户通过访问“单一访问点”即可访问“所有服务器”上提供的资源。

文件服务器用来将网络中的“所有服务器”进行进一步管理，可以提供 “文件夹配额”与“文件屏蔽”功能，可以限制用户使用的共享文件夹的大小以及只能保存“文件服务器”指定的文件。

RRAS 服务器是“路由和远程访问服务器”的简称，可以用作“所有工作站”与“所有服务器”访问 Internet 的代理服务器，也可以用作通过 Internet（或者使用其他方式上网）访问企业内部局域网的“远程访问服务器”，还可以用作“远程访问的路由器”。

7.1.2 交换机规划

在 Microsoft 系列产品中，除了 DHCP 服务器、RIS 服务器和 Windows 部署服务器需要对企业的三层交换机进行配置外，其他的服务器都不涉及三层交换机的配置。如果企业网络中没有使用三层交换机，或者虽然使用了三层交换机，但没有划分 VLAN，同样也不需要对三层交换机进行配置。

如果 DHCP 服务器、RIS 和 Windows 部署服务器在 VLAN 环境中，需要在三层交换机中配置“DHCP 中继”，使其指向 DHCP 服务器、RIS 与 Windows 部署服务器的地址，其他的则不需要配置。

在使用 ISA Server 时，如果涉及到多出口的环境，也需要对三层交换机进行配置，这时候需要配置静态路由。

7.2 将 Windows Server 2008 R2 升级到 Active Directory

从本章开始，介绍使用 Windows Server 2008、Windows Server 2008 R2 的 Active Directory 管理网络的内容。为了统一，本章中服务器的计算机名为 dc，域名为 heinfo.local，IP 地址为 172.30.5.15，子网掩码为 255.255.255.0，DNS 服务器地址为 172.30.5.15。所有工作站地址为 172.30.5.30～172.30.5.200，子网掩码为 255.255.255.0，DNS 服务器地址为 172.30.5.15。

在实际的网络中，如果工作站和服务器需要上网，或者网络中有多个 VLAN，还要正确设置

网关地址，而 DNS 服务器可以通过在服务器 172.30.5.15 上设置 DNS 转发来获得。

如果读者使用 Windows 2008 R2 虚拟机来做这些实验，须将 Windows 2008 R2 的虚拟机的虚拟硬盘“还原”（可以使用 Hyper-V 的“快照”与“还原”功能）。

在将 Windows 2008 R2 虚拟机还原后，须设置计算机的 IP 地址为 172.30.5.15、DNS 为 172.30.5.15（如图 7-2 所示），单击“确定”按钮。修改计算机的名称为 dc（如图 7-3 所示）后，重新启动计算机。

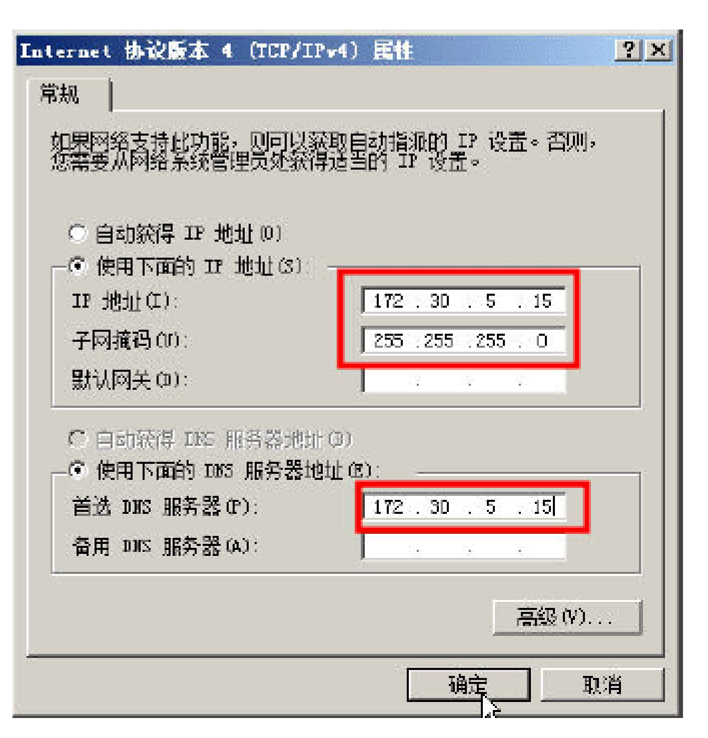


图 7-2　设置 IP 地址与 DNS



图 7-3　修改计算机名称

再次进入 Windows Server 2008 R2 后，以管理员账户（Administrator）登录，执行如下操作。

01 打开“运行”对话框，运行“dcpromo”命令，启动活动目录安装向导，如图 7-4 所示，单击“下一步”按钮。

02 在“选择某一部署配置”对话框，选中“在新林中新建域”单选按钮，单击“下一步”按钮，如图 7-5 所示。

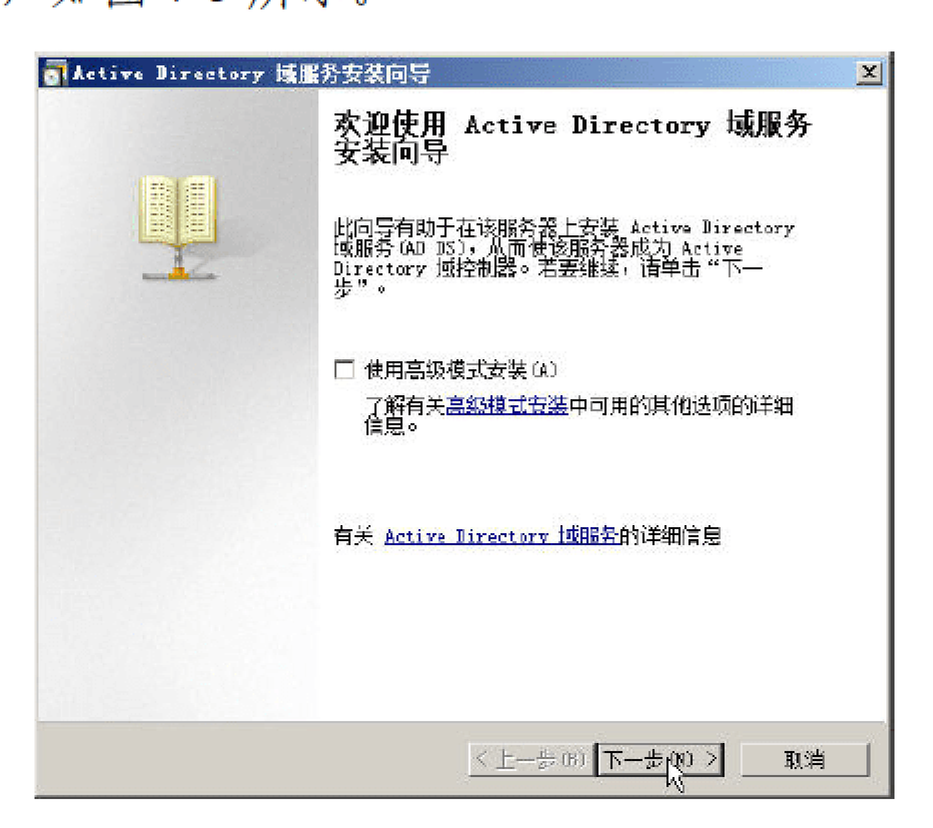


图 7-4　活动目录安装向导



图 7-5　在新林中新建域

03 在“命名林根域”对话框中，在“目录林根级域的 FQDN”文本框中输入已规划的域名 heinfo.local，单击“下一步”按钮，开始检查域名称，如图 7-6 所示。

04 在“设置林功能级别”对话框，选择林功能级别，如果网络中只有 Windows Server 2008 R2 的服务器，则选择“Windows Server 2008 R2”，如果网络中还有 Windows Server 2008 的服务

器，则选择“Windows Server 2008”；如果网络中有 Windows 2003 的服务器，则选择“Windows 2003”；如果网络中有 Windows 2000 的服务器，则选择 “Windows 2000” 。如果选择的是 Windows 2000 或 Windows Server 2003、Windows Server 2008，当网络中的服务器全部升级到 Windows Server 2008 R2 后，可以将“林功能级别”提升到 Windows Server 2008 R2。在本例中，选择 Windows Server 2008 R2，如图 7-7 所示。



图 7-6 DNS 名称

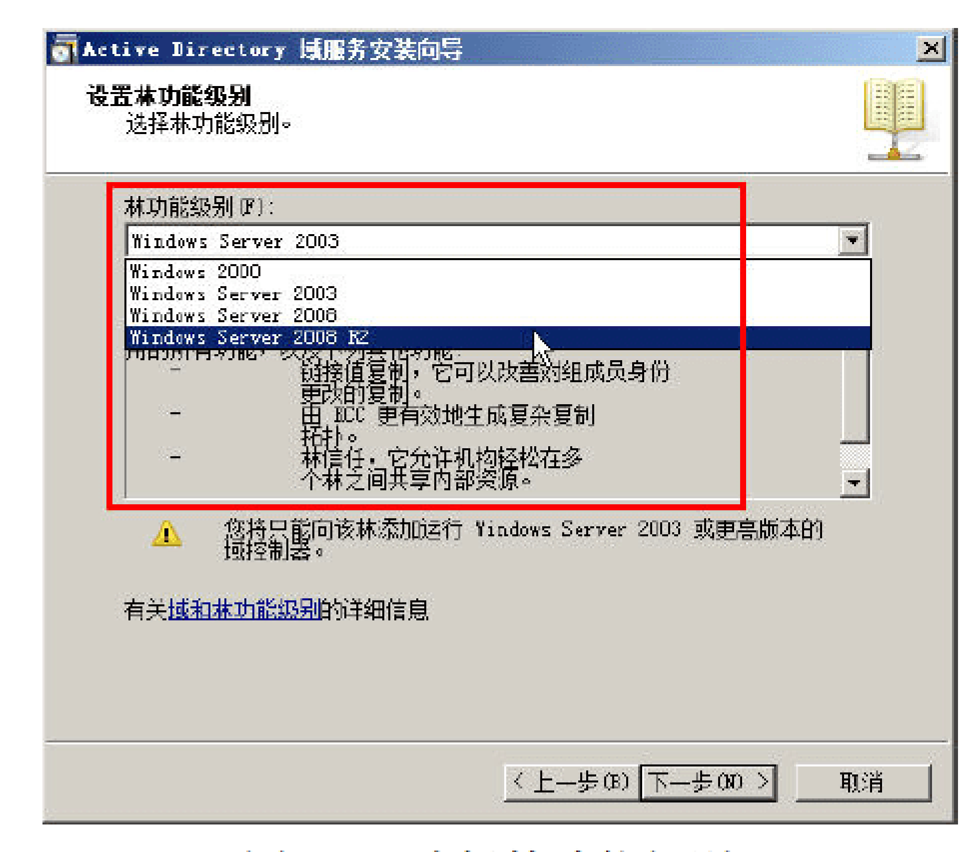


图 7-7 选择林功能级别

05 在“其他域控制器选项”对话框，选中“DNS 服务器”复选框，单击“下一步”按钮，如图 7-8 所示。

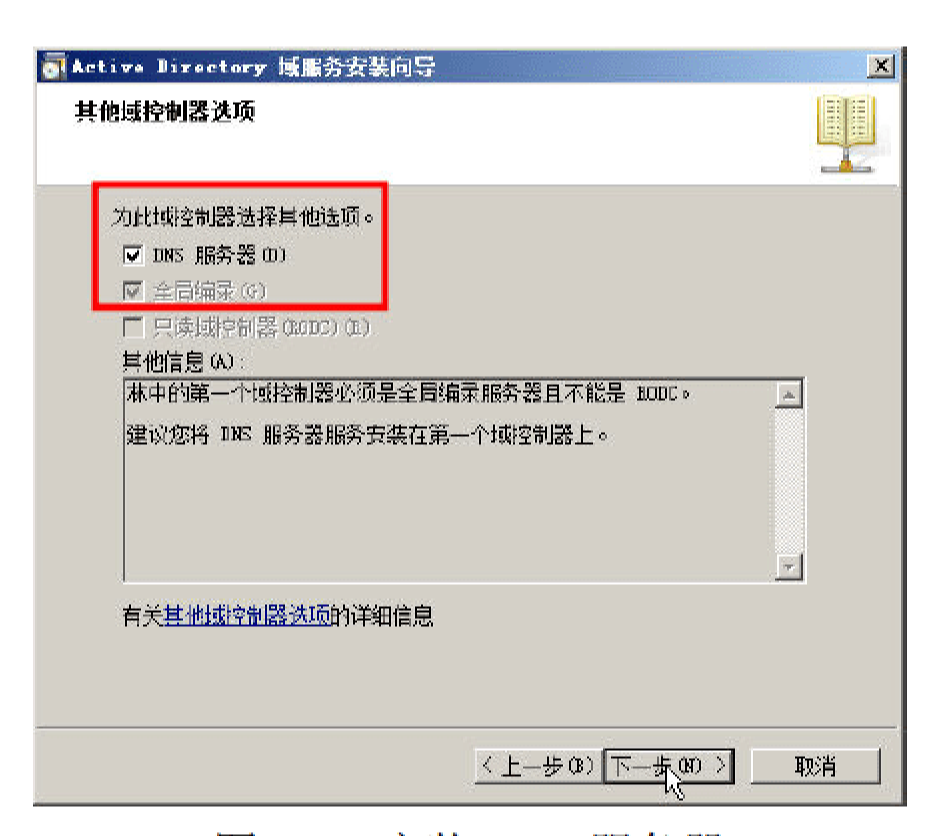


图 7-8 安装 DNS 服务器

06 在“数据库、日志文件和 SYSVOL 的位置”对话框中，指定数据库、日志文件、文件夹对话框，通常选择默认值即可。

07 在“目录服务还原模式的 Administrator 密码”对话框中，设置目录服务还原模式密码如图 7-9 所示。该密码不同于管理员的密码，在使用目录服务还原模式时必须输入。

08 在“摘要”对话框中，检查相关设置是否正确，如图 7-10 所示。确定设置无误后，单击“下一步”按钮，将开始 Active Directory 服务的安装，如图 7-11 所示。

09 安装完成之后，显示如图 7-12 所示。单击“完成”按钮，根据系统提示重新启动 Windows Server 2008 计算机，完成 Active Directory 的安装。

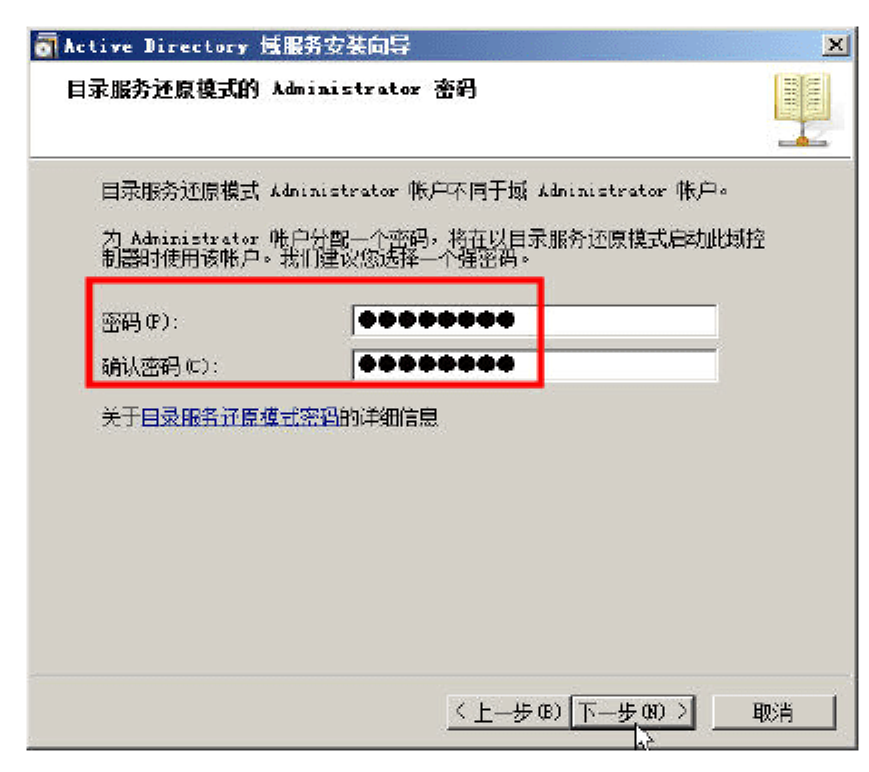


图 7-9　设置目录服务还原模式密码



图 7-10　“摘要”对话框

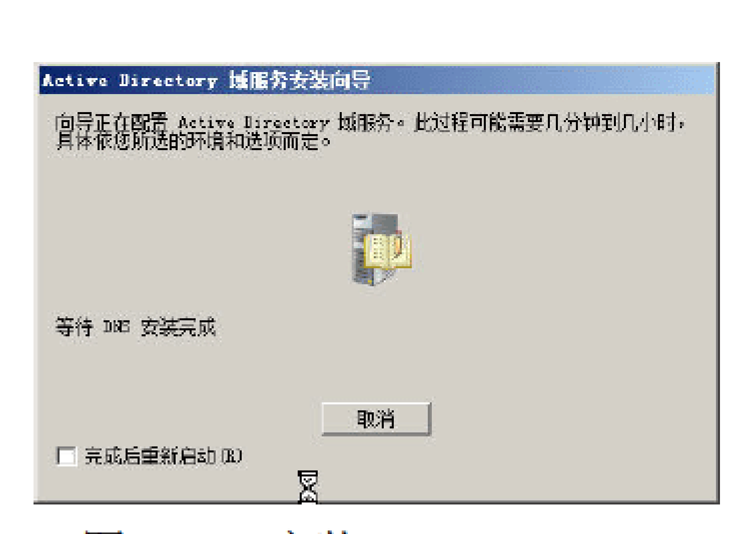


图 7-11　安装 Active Directory

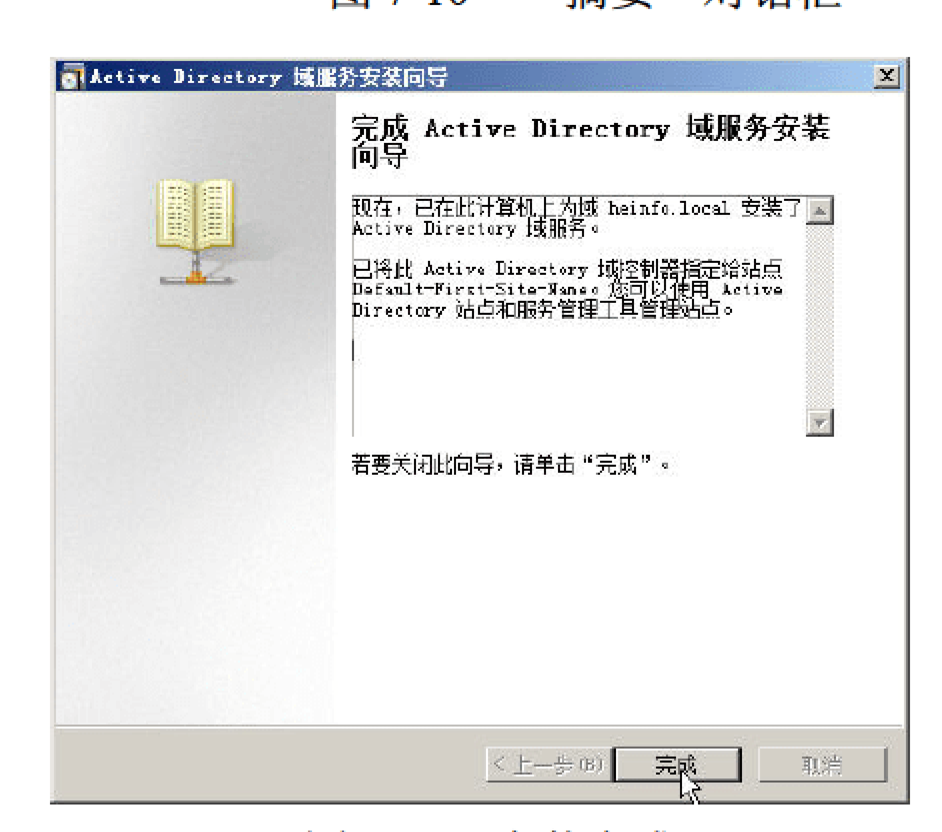


图 7-12　安装完成

7.3　域用户与域用户组管理

计算机是模拟现实生活的电子设备，同样的，联网的计算机也是在模拟客观世界人与人之间的关系与交往。在现实世界中，人人都有一个身份，每个人的身份决定了他的工作与职权范围。而在计算机网络，也有一个代表“身份”的名称，称为“用户”。用户的权限不同，决定了用户对计算机及网络控制的能力与范围也各不相同。用户有两种类型：一种是只能用来访问本地计算机（或使用远程计算机访问本计算机）的“本地用户账户”，另一种是可以访问网络中所有计算机的“域用户账户”。

7.3.1　命名惯例

在企业网络中，使用计算机的每个人都应该有一个用户账户，用户通过他们自己的账户可以使用企业网络中指定的资源，完成与其相对应的任务。除了每个人有一个用户账户外，还可能有为此用户提供的一些对应服务，如企业电子邮件服务、企业办公自动化的登录账户等。所以，通常情况下都是使用统一的方式进行命名，以便于计算机的使用者记住自己的用户名。另外，通常用户名还与企业为其提供的电子邮件相对应（如用户名为 zs，企业电子邮件是 zs@heinfo.local）。

命名习惯通常如下：

- 对于计算机来说，如果计算机是专属于某一个人使用，则以这个人的名字命名计算机，如果计算机是几个人来共用，则以科室的名称命名，如果一个科室中有多台计算机，在命名的时候同时添加序号即可。
- 对于每个使用者，通常都是使用其“姓”的全称 + “名”的简称，如张三的用户名为 zhangs。
- 如果使用简称之后有“重名”的现象，可以对重名的用户使用全称。

7.3.2　密码要求

在以前的 Windows 2000 网络中，对密码是没有强度要求的，用户可以根据习惯是否使用密码，也可以根据习惯使用哪种密码。但随着网络安全被越来越重视，Windows Server 2008 网络对密码有了新要求。用户不仅必须设置和使用自己的密码，而且密码要符合如下要求：

- 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分。
- 至少有 6 个字符长。
- 包含以下 4 类字符中的 3 类字符：
  - 英文大写字母（A～Z）。
  - 英文小写字母（a～z）。
  - 10 个基本数字（0～9）。
  - 非字母字符（例如 !、$、#、%）。

在更改或创建密码时执行复杂性要求。对于“本地用户账户”或修改了 Windows Server 2008 默认组策略的计算机，其用户密码可以随意设置。

将计算机升级到 Active Directory 服务器后，原来的“本地用户和用户组”管理工具将不复存在，而改用“Active Directory 用户和计算机”进行统一的管理，原来的“本地用户”将迁移到 Active Directory 用户中，并具有更多的属性。

Active Directory 的用户可以在其所属的整个网络或与其建立了信任关系的网络中使用。

7.3.3　创建域用户账户

本小节介绍如何创建域用户账户，操作步骤如下。

01 以管理员身份（Administrator 账户）登录服务器，从“管理工具”中打开“Active Directory 用户和计算机”控制台，如图 7-13 所示。在“Active Directory 用户和计算机”中的 heinfo.local（域名）下的“Users”中保存域中的用户组和用户。可以在“Users”中创建新的用户和用户组，也可以在 heinfo.local 域下面创建 OU（组织单元），再在 OU 中创建用户或用户组。

02 在“Users”右侧的空白窗格中右击，或者选中“Users”右击，从快捷菜单中选择“新建→用户”选项，打开“新建对象-用户”对话框，如图 7-14 所示。在“姓名”文本框输入要创建的用户名如 ws01，在“用户登录名”文本框输入 ws01，其他可以不输入。

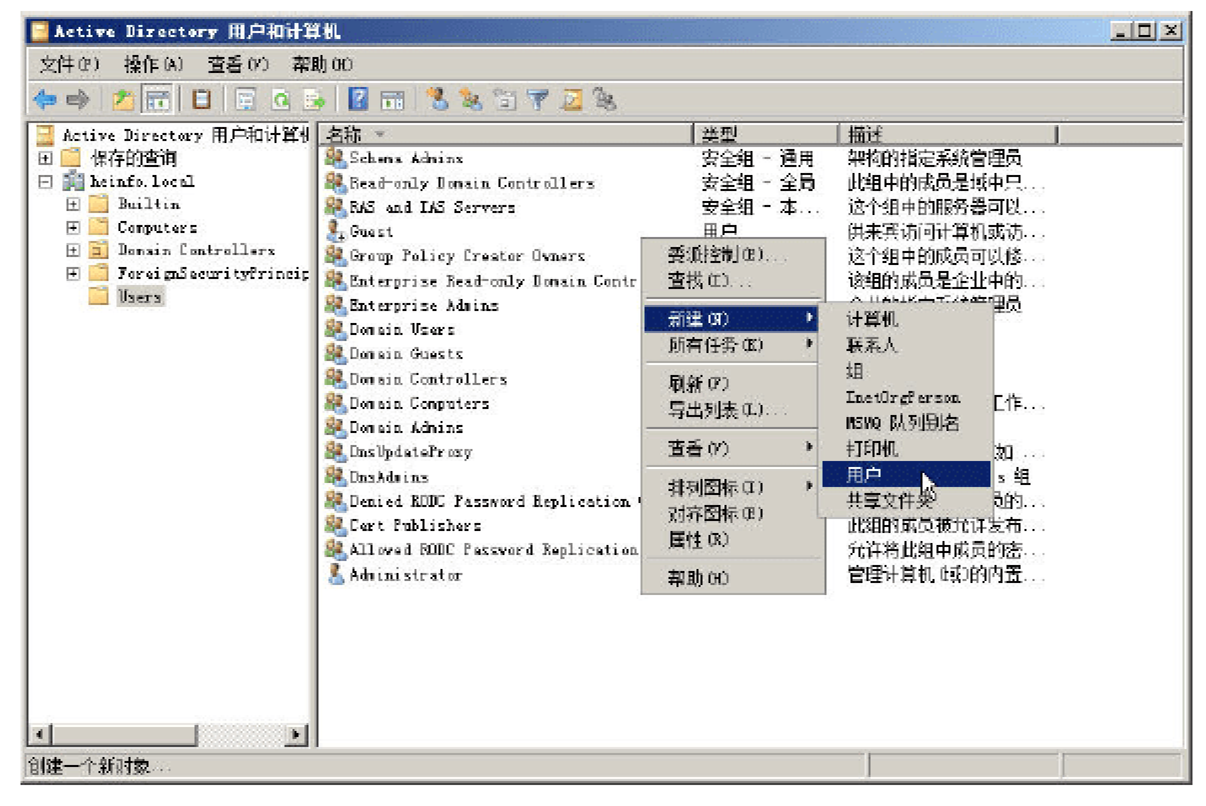


图 7-13 Active Directory 用户和计算机

03 单击“下一步”按钮，显示如图 7-15 所示对话框，需要设置密码与基本用户属性对话框。在“密码”与“确认密码”文本框输入新密码（注意，用户密码必须符合 Windows 强密码的要求，详情参见“7.3.2 密码要求”的内容），根据实际情况设置用户的登录属性，

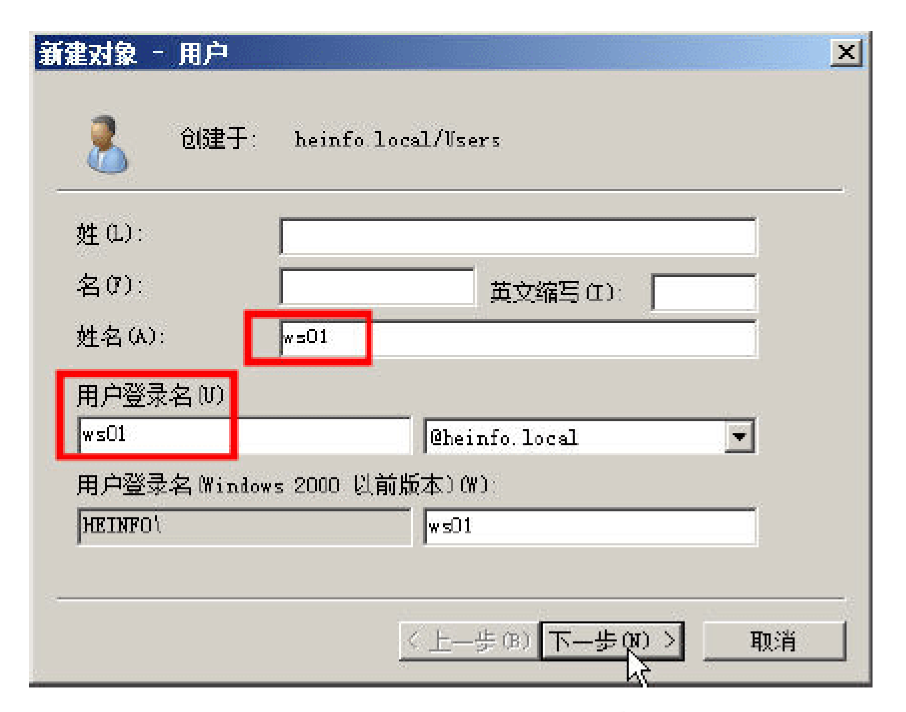


图 7-14 创建用户

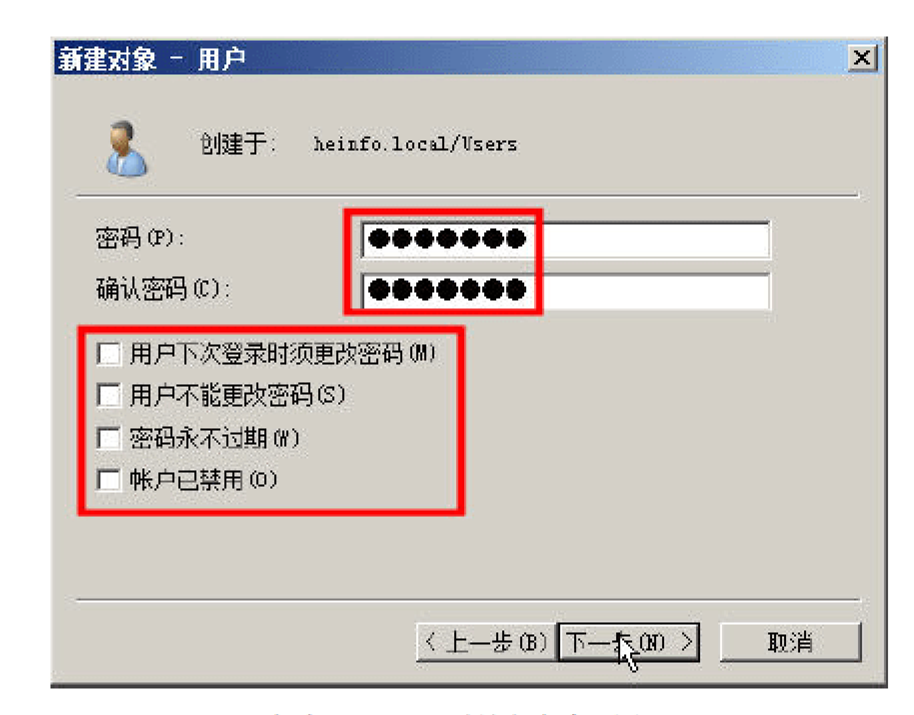


图 7-15 设置密码

04 单击“下一步”按钮，创建用户完成，如图 7-16 所示。如果设置的用户密码符合 Windows 要求，单击“完成”按钮后将会返回 Active Directory 用户和计算机；如不符合要求，则会显示如图 7-17 所示对话框。此时可返回并重新设置符合要求的密码，再继续创建用户。

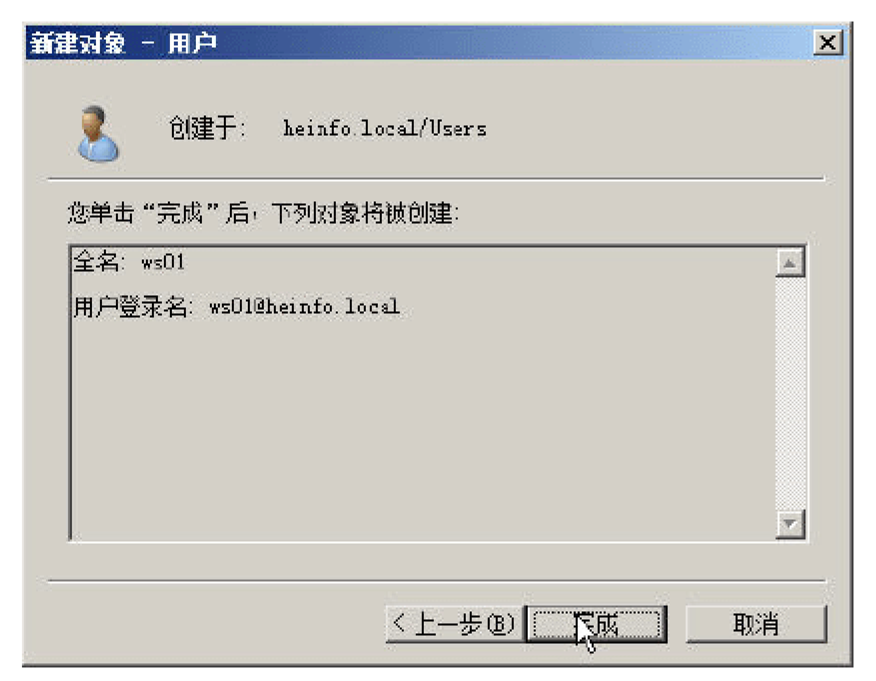


图 7-16 创建用户完成

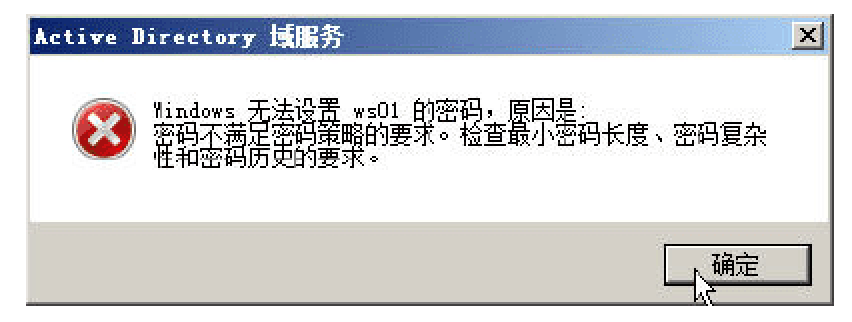


图 7-17 密码不符合要求

7.3.4 设置域用户账户的属性

域用户账户除了具有“本地用户账户”的全部属性外，还具有一些其他的属性，如用户的地址、电话、单位等信息，还可以设置用户的登录时间、登录到的计算机等信息。本节将介绍怎样设置用户的登录时间和登录到的计算机。

1. 设置登录时间

如果要设置账户的登录时间，可以按照如下的步骤操作。

01 选择欲设置登录时间的用户，右击并选择快捷菜单中的“属性”选项，打开用户属性对话框，如图 7-18 所示。

02 选择“账户”选项卡，单击“登录时间”按钮，打开登录时间设置对话框，如图 7-19 所示。默认允许登录时间是全部。可以设置的登录时间是按星期一到星期日、每天 24 个小时，每小时一个设置区间来划分的。用鼠标选中区域，选中“允许登录”或“拒绝登录”单选按钮即可设置为允许或拒绝登录。如图 7-20 所示为设置每星期一到星期五的 8:00~18:00 和星期六的 18:00~24:00 允许登录，其他时间则不允许。

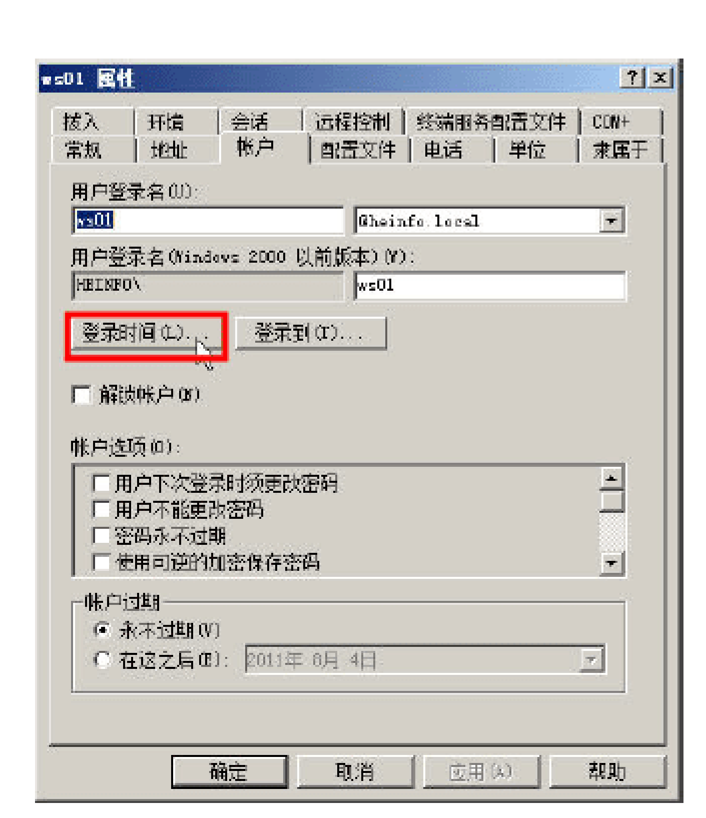


图 7-18 用户属性对话框

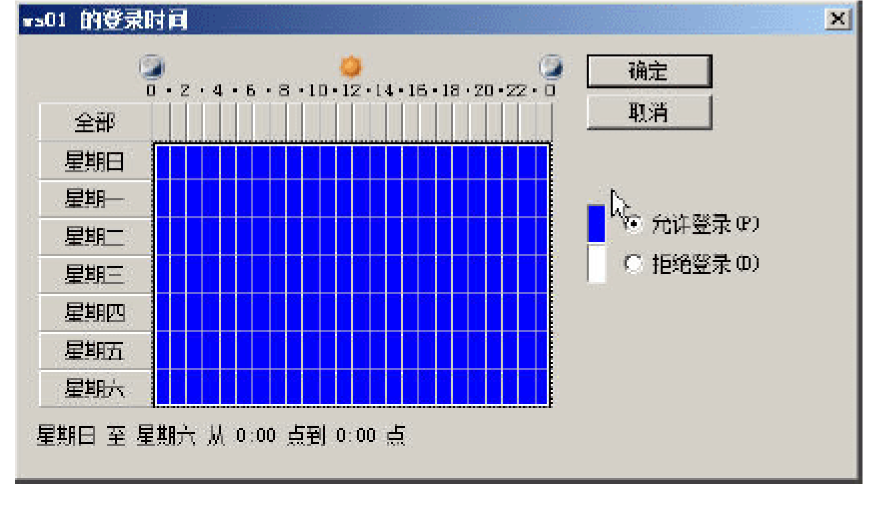


图 7-19 登录时间设置

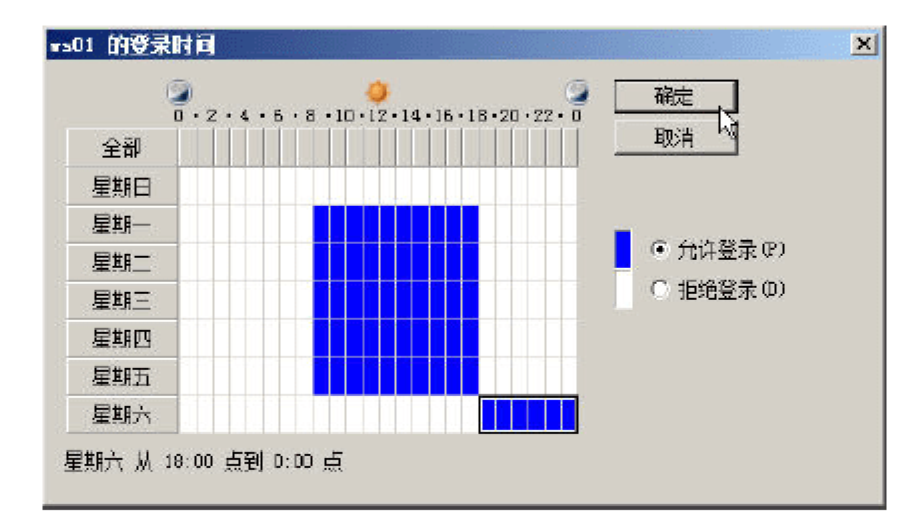


图 7-20 登录时间

03 设置完成后单击“确定”按钮返回。

2. 设置登录到的计算机

如果指定账户，在指定的计算机登录，可以按照如下方式设置。

01 在用户属性对话框的“账户”选项卡中，单击“登录到”按钮（参考图 7-18 所示），显示“登录工作站”对话框，如图 7-21 所示。默认选中“所有计算机”单选按钮，允许该用户登录到所有计算机。

02 如果要设置允许登录的计算机，可选中“下列计算机”单选按钮，在“计算机名称”文本框输入允许此用户登录到的计算机名，单击“添加”按钮添加到列表中即可。可以在列表中添加多台计算机，如图 7-22 所示。

03 单击“确定”按钮保存设置并返回。

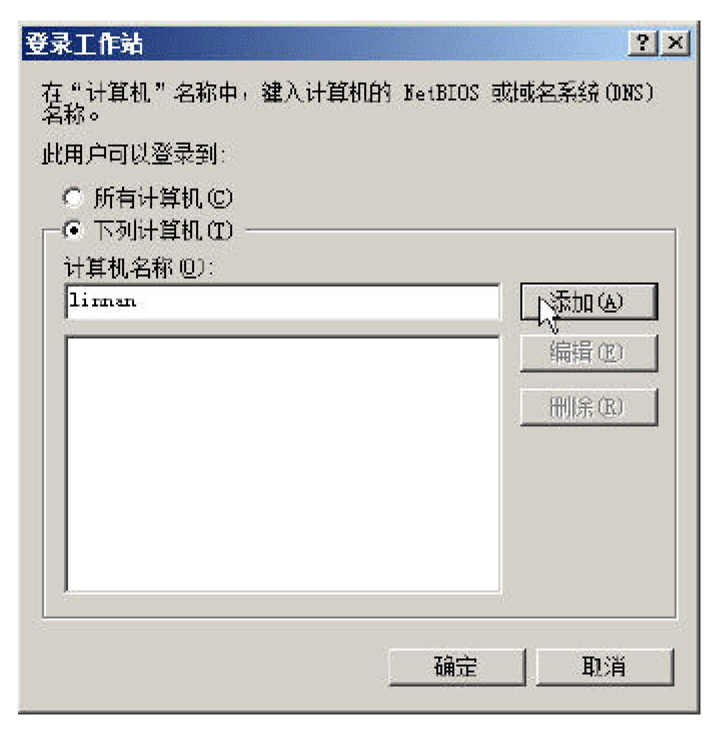


图 7-21　登录到计算机

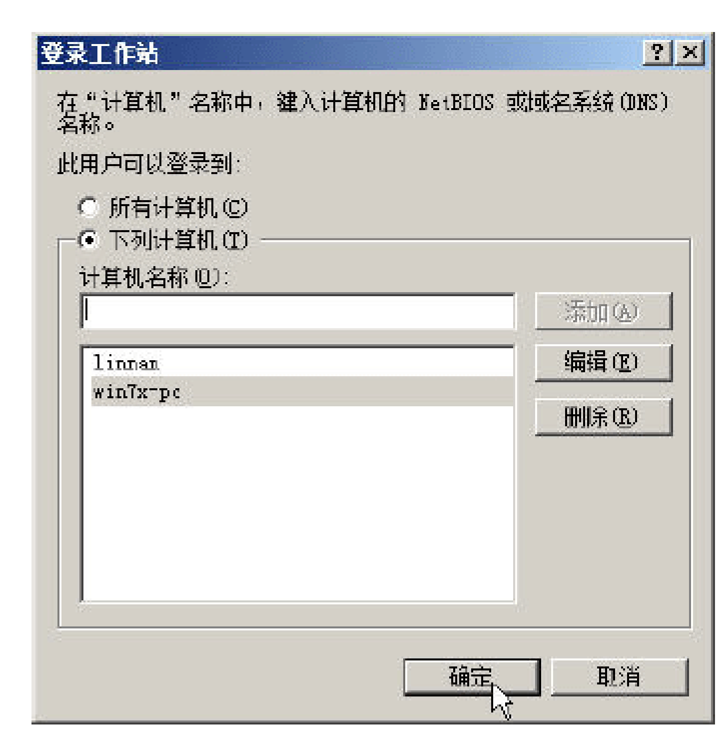


图 7-22　添加计算机

7.3.5　其他操作

在"Active Directory 用户和计算机"窗口中，选中一个用户，右击，将显示快捷菜单，如图 7-23 所示，可以完成添加到组、禁用账户、重置密码、移动、复制、打开主页、发送邮件、删除和重命名等操作。

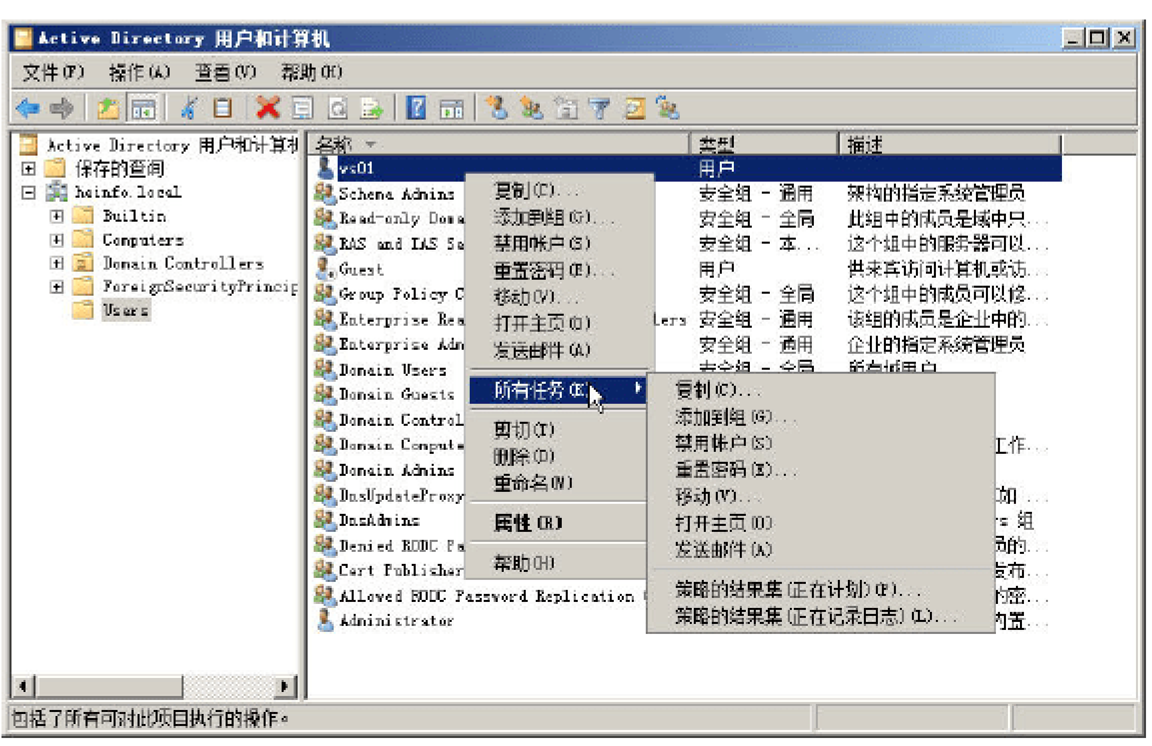


图 7-23　快捷菜单

（1）添加到组

如果在快捷菜单中选择"添加到组"命令，将显示如图 7-24 所示"选择组"对话框，可以将用户添加到其他用户组中。

（2）禁用账户

如果在快捷菜单中选择"禁用账户"命令，将会禁用此账户登录。

（3）重置密码

在快捷菜单中选择"重置密码"命令，可以重新设置用户的密码，如图 7-25 所示。

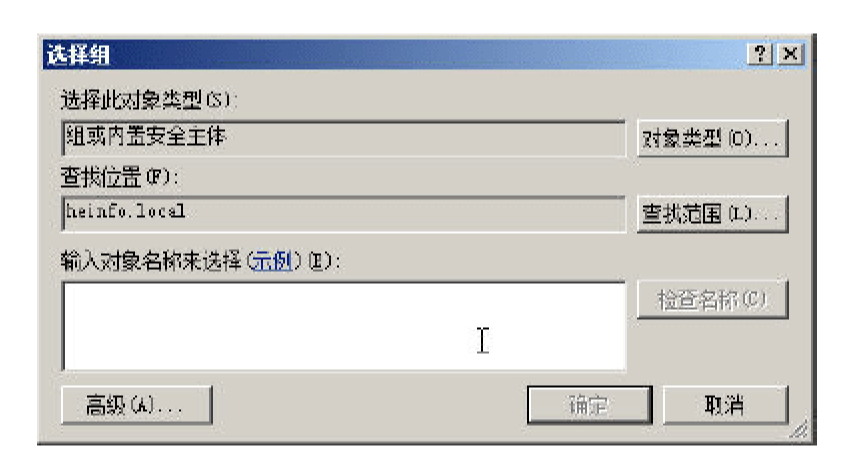


图 7-24　将用户添加到组

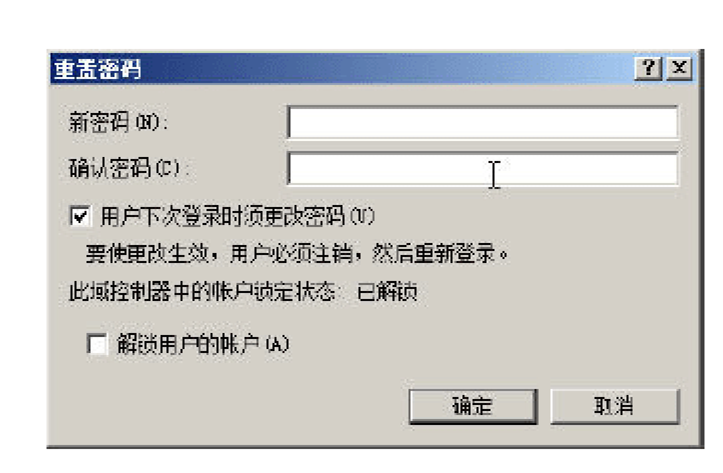


图 7-25　重置密码

（4）移动

在快捷菜单中选择“移动”命令，可以把用户移动到另一个组中，如图 7-26 所示。

（5）复制

如果在快捷菜单中选择“复制”命令，显示如图 7-27 所示“复制对象-用户”对话框。输入新用户的信息（用户名、登录名），单击“下一步”按钮，显示设置密码对话框，设置密码之后，复制用户完成。系统将创建一个与选择用户的属性相同的用户。



图 7-26　移动对象

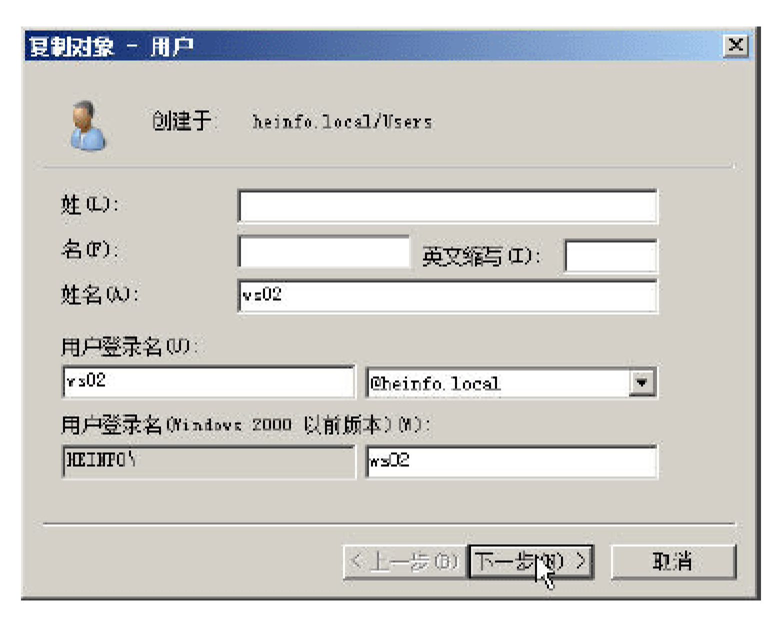


图 7-27　复制用户

复制的用户具有与被复制用户相同的权限及所属用户组。

（6）打开主页或发送邮件

如果选择快捷菜单中的“打开主页”命令，将会打开用户的主页。选择快捷菜单中的“发送邮件”命令，将会向此用户发送邮件。使用这两项的前提是：已经在用户的属性中进行了相应的设置。

（7）删除

选择快捷菜单中的“删除”命令，将删除所选择的用户。

（8）重命名

选择快捷菜单中的“重命名”命令，可以更改被选择用户的显示名称。

7.3.6 创建域用户组

在“Active Directory 用户和计算机”窗口中，选择“Users”，在右侧的空白窗格中右击，显示如图 7-28 所示的快捷菜单，选择“新建→组”命令，显示新建用户组对话框，如图 7-29 所示。

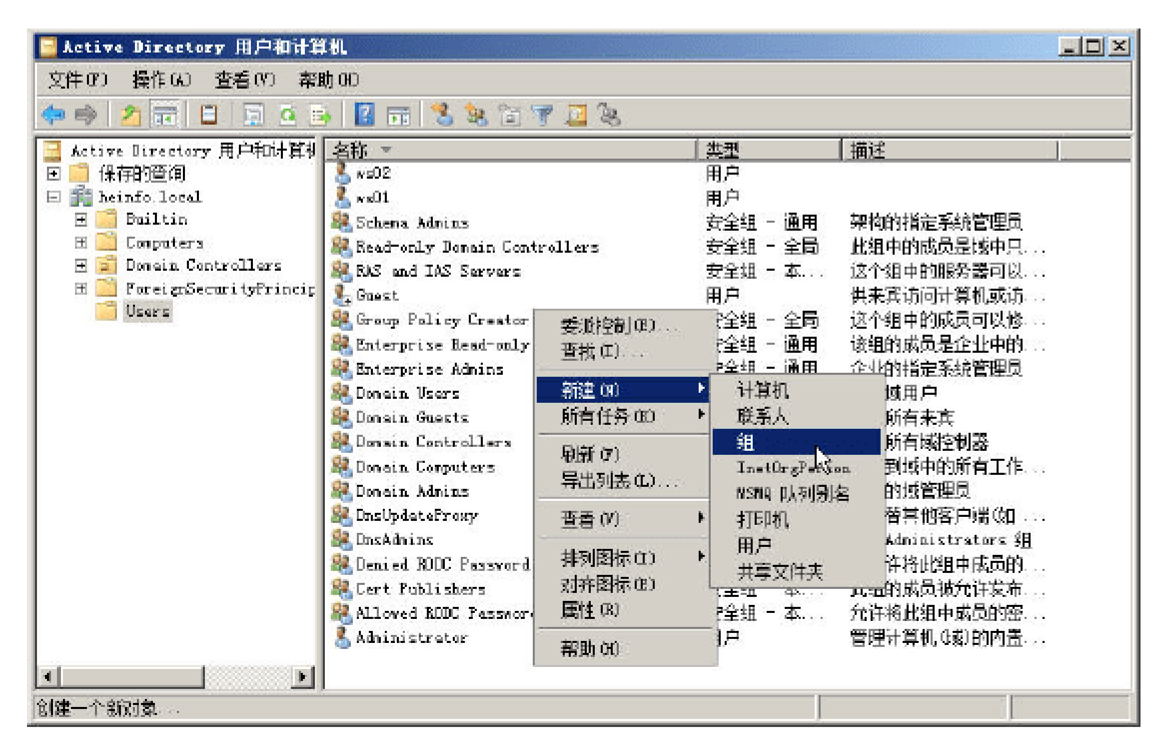


图 7-28　新建组

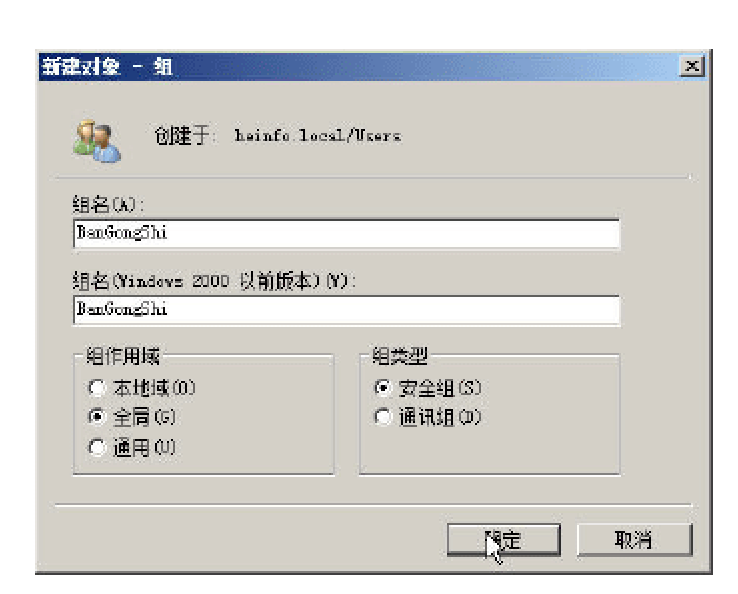


图 7-29　新建用户组

在“组名”及“组名（Windows 2000 以前版本）”文本框中输入组名，从“组作用域”和“组类型”选项区域中选择合适的类型，单击“确定”按钮即完成用户组的创建。

7.4　OU 的规划

包含在域中的特别有用的目录对象类型就是组织单位（OU）。组织单位是一种 Active Directory 容器，可以将用户、组、计算机和其他组织单位放入其中，但不能容纳来自其他域的对象。组织单位可以指派组策略设置，或者委派管理权限。组织单位代表了域的逻辑层次结构，根据组织的模型管理账户和资源的配置以及使用。不过，不推荐在“Users 容器”中创建用户和用户组，在域中创建组织单位并添加用户较好。

7.4.1　创建 OU

打开“Active Directory 用户和计算机”窗口，选择当前的域，如图 7-30 所示，用鼠标右击，从快捷菜单中选择“新建→组织单位”命令，显示新建组织单位对话框，如图 7-31 所示。输入组织的单位名称（本例为“信息技术学院”），单击“确定”按钮完成创建。

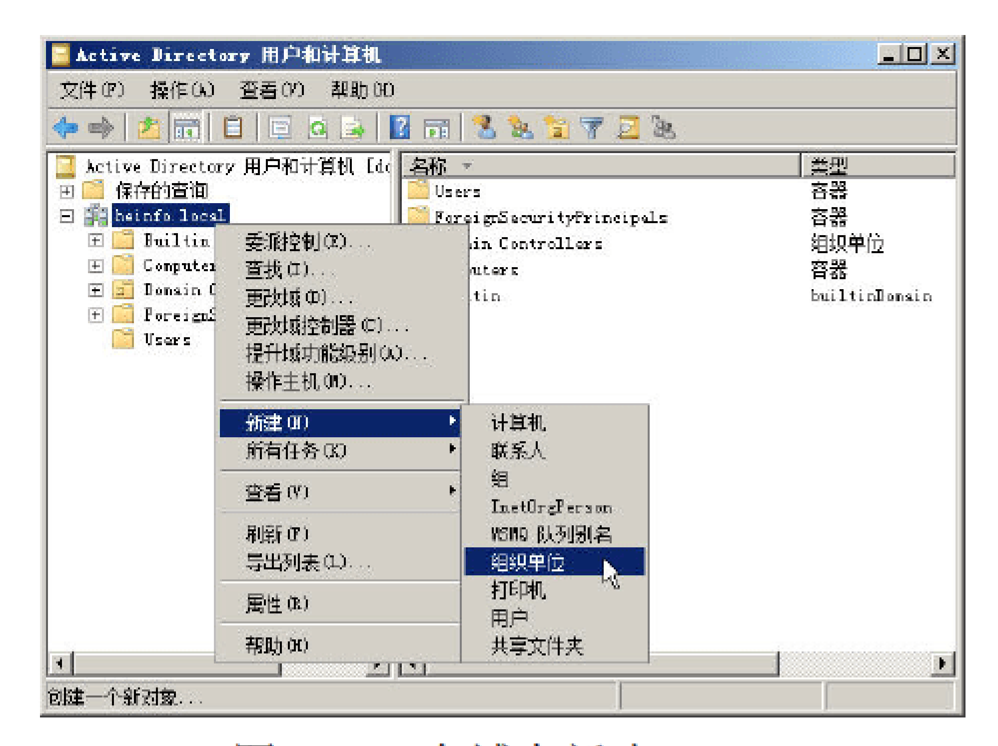


图 7-30　在域中新建 OU

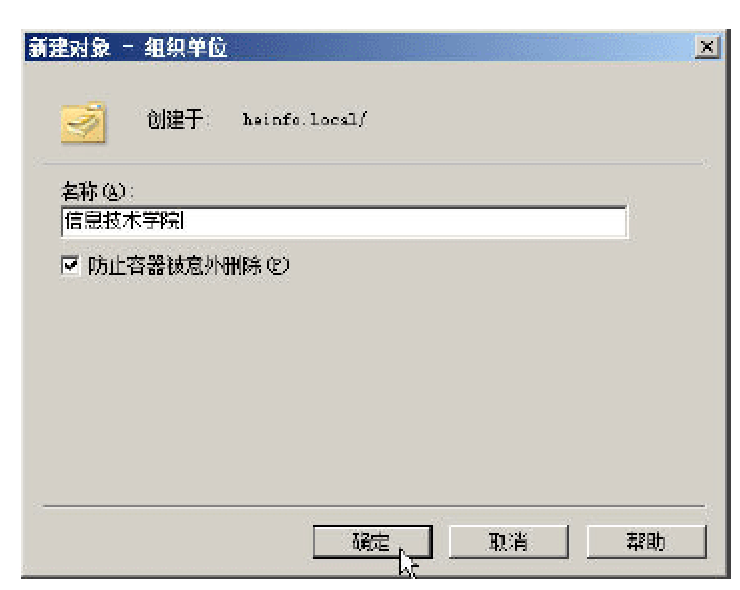


图 7-31　设置 OU 名称

选择新建的组织单位，在右侧的空白窗格中右击，可以在组织单位中继续创建子组织单位，如图 7-32、图 7-33 所示。

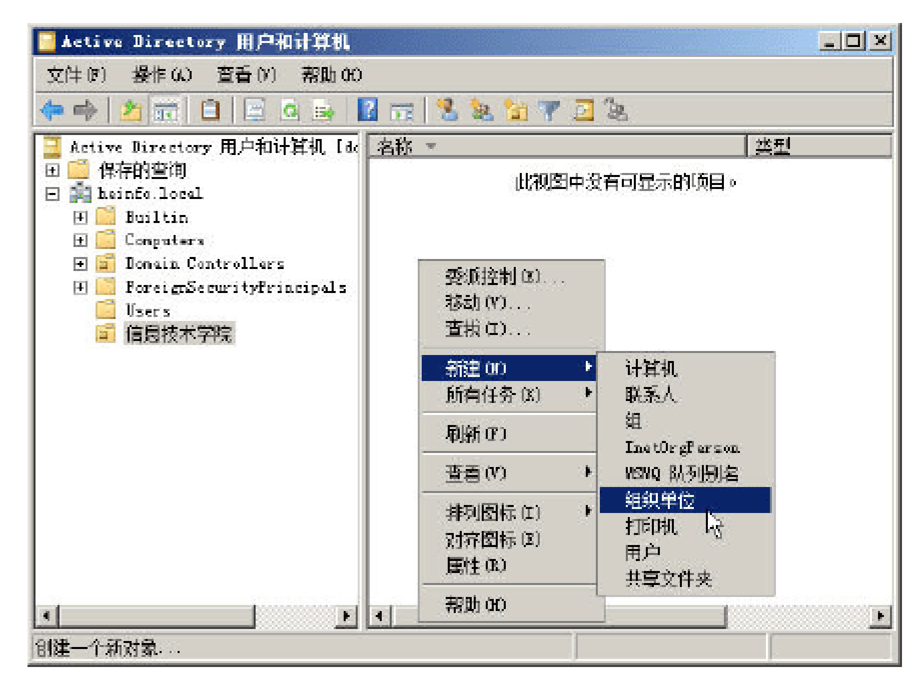


图 7-32　新建子 OU

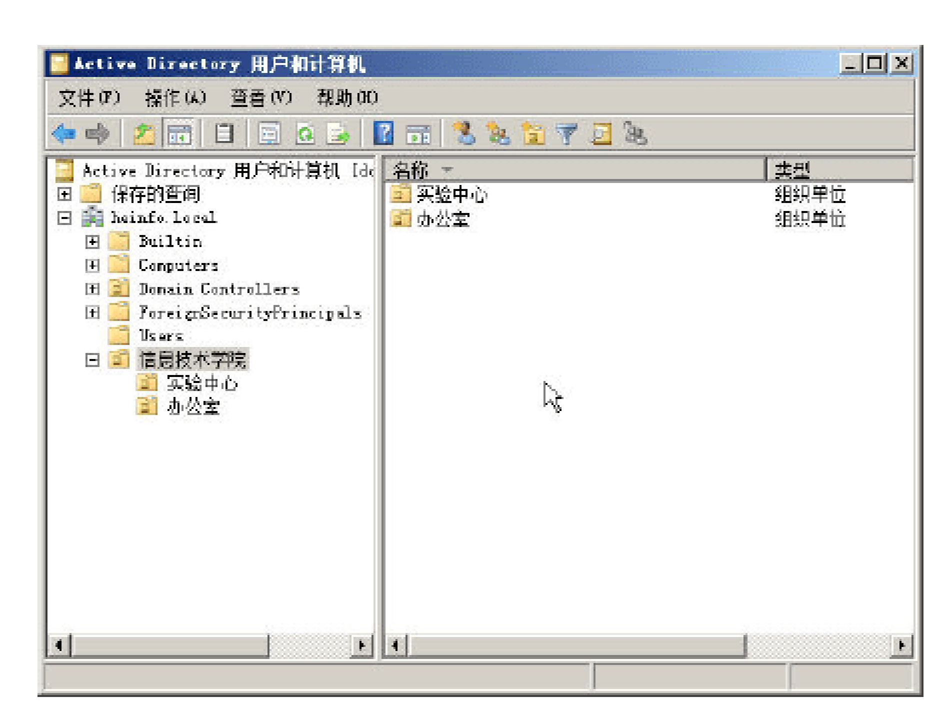


图 7-33　创建子 OU

按照企业结构创建完组织单位后，就可以将以前创建的用户“移动”到其相应的组织单位中以利于管理。Windows Server 2008 正是依靠组织单位及组策略，才能实现许多“自动化”的高级管理功能。

7.4.2 创建大量用户的方法

作为管理员，一个基本的任务就是“创建用户”。虽然创建用户的步骤很简单，但如果需要创建几十个、几百个甚至上千个用户时，就会非常麻烦了。在本小节中，将介绍批量创建用户的方法。NET 是一个很常用的网络命令，使用 NET USER 命令就可以创建大量用户。NET USER 命令的语法如下：

```
NET USER
[username [password | *] [options]] [/DOMAIN]
username {password | *} /ADD [options] [/DOMAIN]
username [/DELETE] [/DOMAIN]
```

语法意义如下：

NET USER ：用于创建和修改计算机上的用户账户。当不带选项使用本命令时，它会列出计算机上的用户账户。

- username ：指需要进行添加、删除、修改或者浏览的用户账户的名字。用户账户的名字不能超过 20 个字符。
- password ：分配或改变用户账户的密码。密码必须满足 NET ACCOUNTS 命令的 /MINPWLEN 选项指定的最小长度的要求。它至多可以具有 14 个字符。 * 表示提示输入密码。当用户在密码提示符下输入时，密码是不会显示的。
- /DOMAIN: 在当前域的主域控制器上执行操作。
- /ADD: 将用户账户添加到用户账户数据库中。
- /DELETE: 从用户账户数据库中删除用户账户。

Options 选项如下所示：

/ACTIVE:{YES | NO} 激活或停用账户。如果账户处于停用状态，用户就不能访问该服务器。该选项的默认值是 YES。

/COMMENT:"text" 提供关于用户账户的一个描述性注释。需要将文本括在引号中。

/COUNTRYCODE:nnn 使用操作系统的国家/地区代码，来实施用户的帮助和错误消息的特定语言文件。0 表示默认的国家/地区代码。

/EXPIRES:{date | NEVER} 如果日期被设置，就会引起账户过期。设置为 NEVER，对账户就没有时间上的限制。根据国家/地区代码的不同，有效日期的格式可以是月/日/年或日/月/年。月可以是一个数字，拼写完整的或三个字母的缩写。年可以是两位或四位数字。使用斜线（/）（没有空格）来分隔日期的各个部分。

/FULLNAME:"name" 是一个用户的完整名字（而不是用户名）。需要把名字用引号括起来。

/HOMEDIR:pathname 设置用户的主目录的路径。路径必须已经存在。

/PASSWORDCHG:{YES | NO} 指定用户是否可以改变自己的密码。其默认值是 YES。

/PASSWORDREQ:{YES | NO} 指定用户的账户是否必须具有密码。其默认值是 YES。

/PROFILEPATH[:path] 为用户的登录配置文件设置路径。

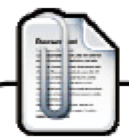
/SCRIPTPATH:pathname 指用户的登录文件所在的位置。

/TIMES:{times | ALL} 指用户可以登录的时间。TIMES 的表达方式是 day[-day][，day[-day]]，time[-time][，time[-time]]，增量限制在 1 小时。天可以是全部拼写或缩写。小时可以是 12 小时或 24 小时制。对于 12 小时制，可以使用 AM，PM。ALL 表示用户总是可以登录。空值表示用户永远不能登录。可以使用逗号分隔天和时间项，并用分号分隔多个天和时间项。

/USERCOMMENT:"text" 让管理人员添加或改变账户的用户注释。

/WORKSTATIONS: {computername[，...] | *}列出至多 8 台用户可以登录到网络上的计算机。如果 /WORKSTATIONS 没有列表或列表是 *，用户就可以从任何一台计算机上登录。

NET HELP command | MORE 用于逐屏显示帮助。



说 明

该命令必须注意空格的使用。各个参数之间（username 也是一个参数）要有空格；同一个参数内，不能用空格隔断，除非空格在引号内。

如果要在没有升级到域控制器的 Windows Server 2008、Windows 7、Windows Server 2003、Windows XP 中创建 3 个用户，最简单的方法是创建如下的批处理文件：

```
net user w11 /add
net user ab2 /add
net user ce3 /add
```

然后运行这个批处理文件，将创建 3 个用户。

如果要在域控制器上，使用 net user 命令创建用户，则需要为用户指定密码，例如，在下面的例子中，将创建 ws11～ws133 个用户、设置用户密码为 a1b2c3D4：

```
net user ws11 a1b2c3D4 /add /domain
net user ws12 a1b2c3D4 /add /domain
net user ws13 a1b2c3D4 /add /domain
```

执行命令的结果如图 7-34 所示。

在使用 net user 创建命令之后，返回到“Active Directory 用户和计算机”窗口，在“Users”组织单位中，选中创建的用户，并“移动”到合适的 OU 中即可，如图 7-35 所示。

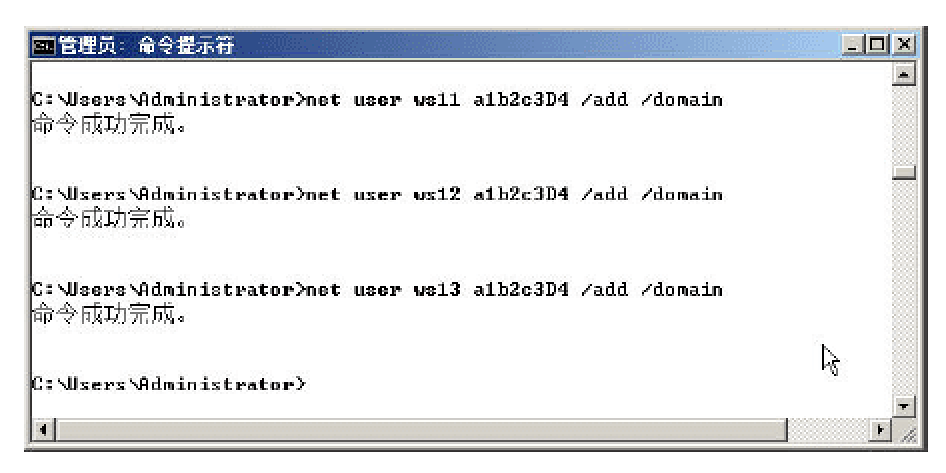


图 7-34　使用 net user 创建用户

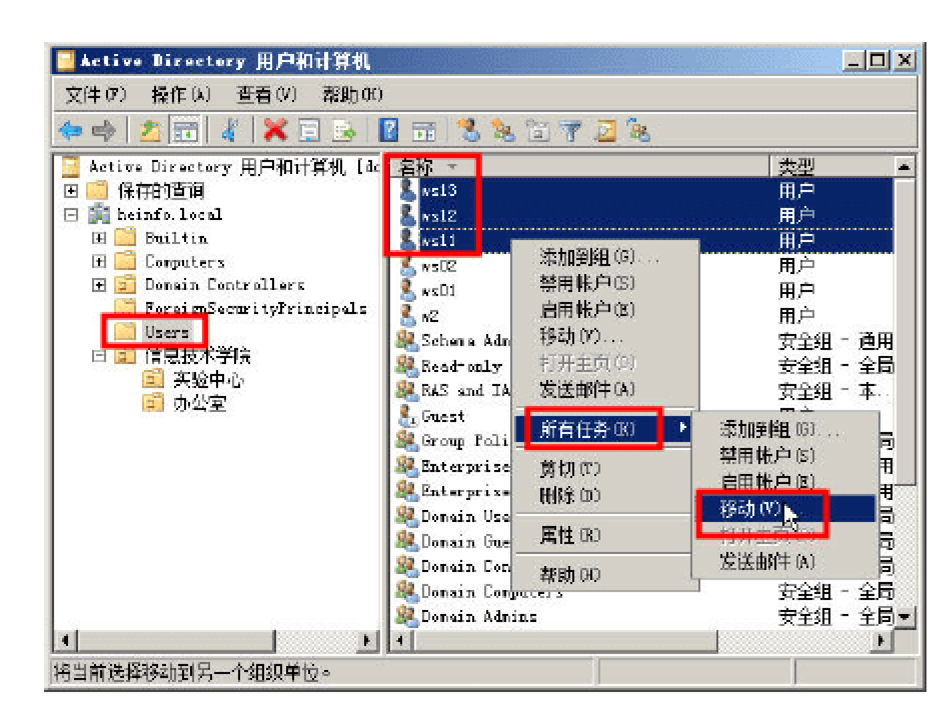


图 7-35　移动用户

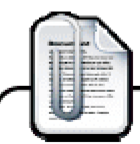
7.5 将 Windows 计算机加入到 Active Directory

只有将计算机加入到域之后，才能使用 Active Directory 进行统一管理。通常来说，并不是所有的 Windows 操作系统都可以加入到 Active Directory（域），只有以下版本的 Windows 才可以将计算机加入到域：

- Windows 2000 ：Professional（专业版）、Server（服务器版）、Advanced Server（高级服务器版）。
- Windows XP: Professional（专业版）。
- Windows Vista: Business（商业版）、Enterprise（企业版）、Ultimate（旗舰版）。
- Windows 7: Professional（专业版）、Enterprise（企业版）、Ultimate（旗舰版）。
- Windows 2003、Windows Server 2008、Windows Server 2008 R2: 除 Web 版以外的所有版本。

通常来说，Windows Server 2003 服务器操作系统对应的客户端是 Windows XP，Windows Server 2008 对应的客户端是 Vista，Windows Server 2008 R2 对应的客户端是 Windows 7。但这些并没有非常严格的限制，通常来说，在 Windows 网络中，可以使用高版本的工作站操作系统加入到低版本服务器的操作系统中，但可能有些“高级功能”不被支持。

在将工作站加入到域的过程中，Windows XP 的操作与 Windows 2000、Windows Server 2003 类似；Windows 7 的操作与 Windows Vista、Windows Server 2008、Windows Server 2008 R2 类似。所以将以 Windows XP、Windows 7 这两个版本为例进行介绍。



说 明

请使用 Virtual PC 2007 创建两台虚拟机，分别安装 Windows XP Professional 与 Windows 7 旗舰版，并且与 Windows 2008 使用相同的虚拟网卡（例如都使用“内部网络”或“NAT 网络”）。

7.5.1 将 Windows XP 计算机添加到域

首先以 Windows XP Professional 为例，添加到域的步骤如下。

01 以本地管理员账户登录计算机，修改每一台工作站的 DNS 地址，将其设为 Active Directory 域控制器的 IP 地址，在本例中，设置 Windows XP 的工作站的 IP 地址为 172.30.5.31，DNS 为 172.30.5.15，如图 7-36 所示。

02 在加入到域之后，最好是修改工作站的计算机名称，在修改计算机名称之后，重新启动计算机，例如，在本例中，修改工作站的计算机名称为 XP-WS，如图 7-37 所示。

03 再次进入 Windows XP 后，右击“我的电脑”图标，从快捷菜单中选择“属性”选项，显示“系统属性”对话框。选择“计算机名”选项卡，在“计算机名”选项卡中单击“更改”按钮，显示“计算机名称更改” 对话框。在“隶属于”选项组中选中“域”单选按钮，输入域名（本例中为 heinfo.local），如图 7-38 所示。

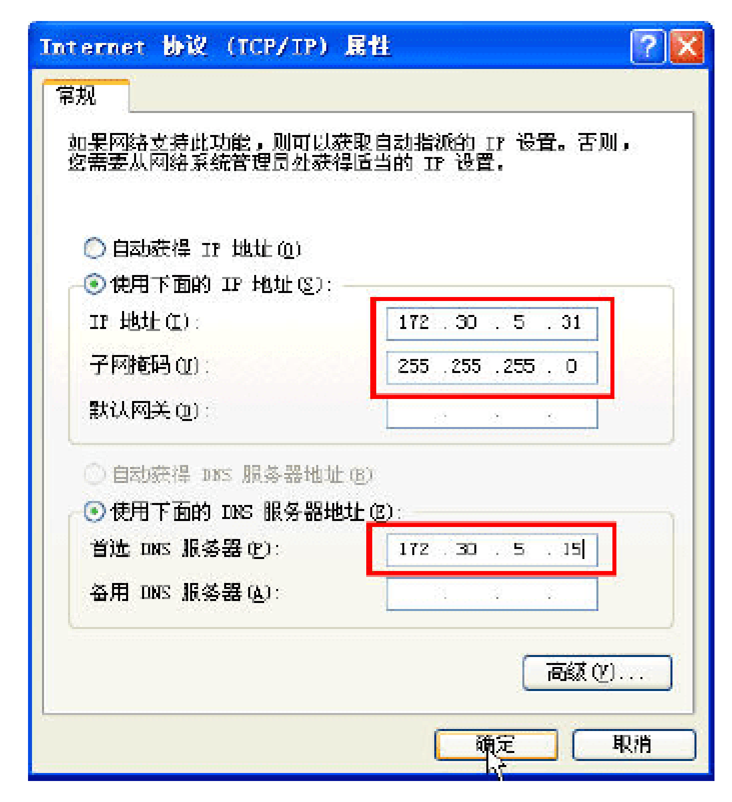


图 7-36　设置 IP 地址与 DNS

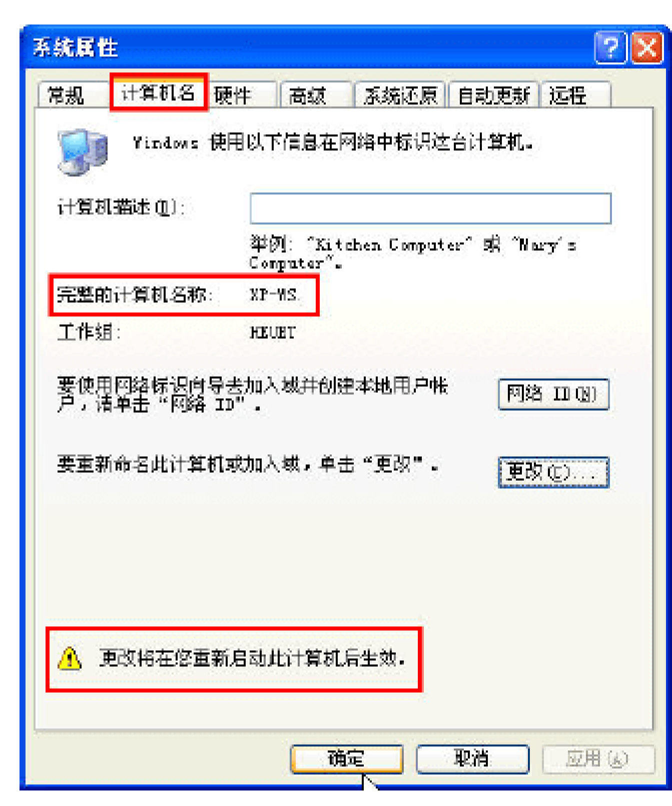


图 7-37　修改计算机名称

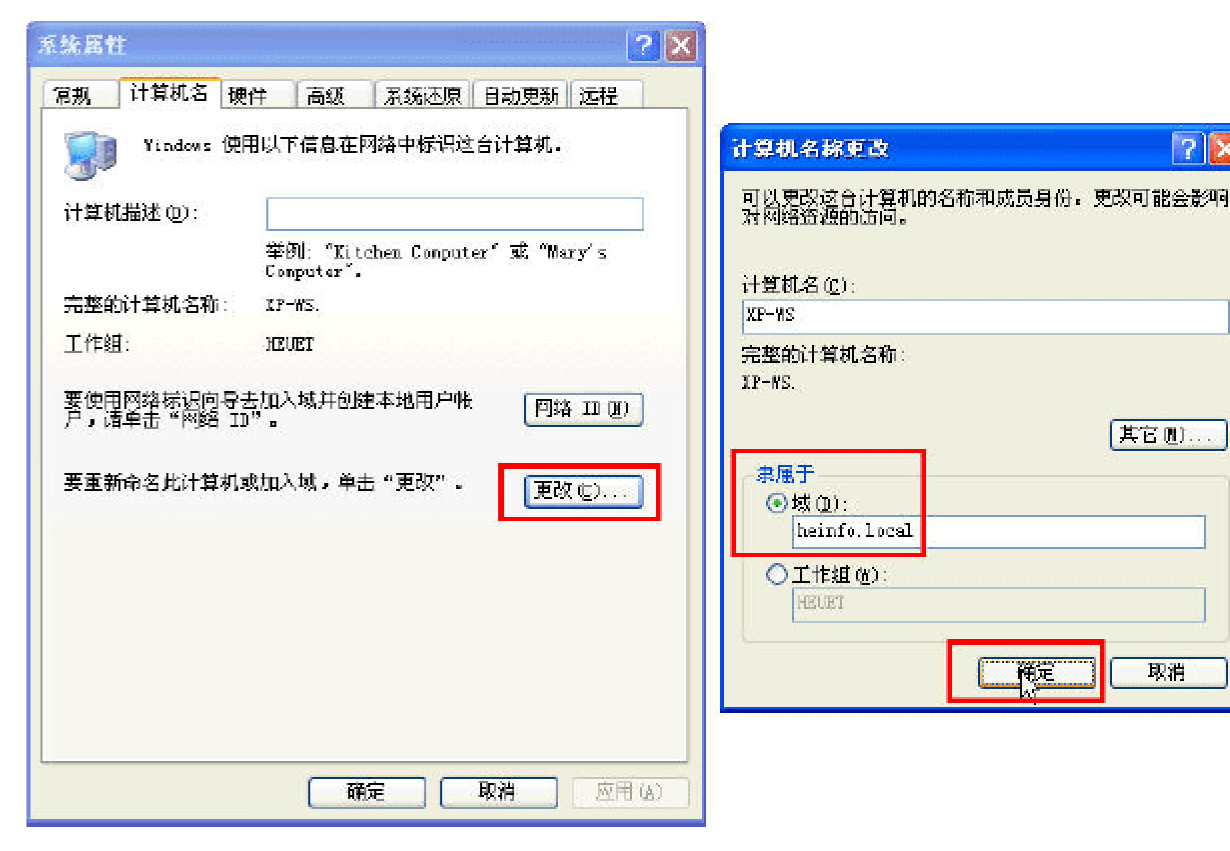


图 7-38　输入域名

04 单击“确定”按钮，显示登录对话框，输入域用户管理员或委派的具有将计算机添加到域权限的用户名和密码，在此先输入域管理员账户 administrator 及域管理员密码（如图 7-39 所示），在以后的章节中，我们将介绍怎样“委派”普通用户具有“将计算机加入到域”的权限。

05 单击“确定”按钮，加入域成功，提示“欢迎加入 heinfo.local 域”，如图 7-40 所示。



图 7-39　输入与用户名和密码



图 7-40　加入域成功

加入到域之后，根据提示，重新启动计算机。

06 以后再登录 Windows XP 时，在“登录到”后面选择 HEINFO 域，输入域用户名、密码即可登录，如图 7-41 所示。在本例中，输入域管理员账户、密码，登录到 Windows XP。



说 明

稍后会介绍怎样用“域普通账户”登录到 Windows XP。

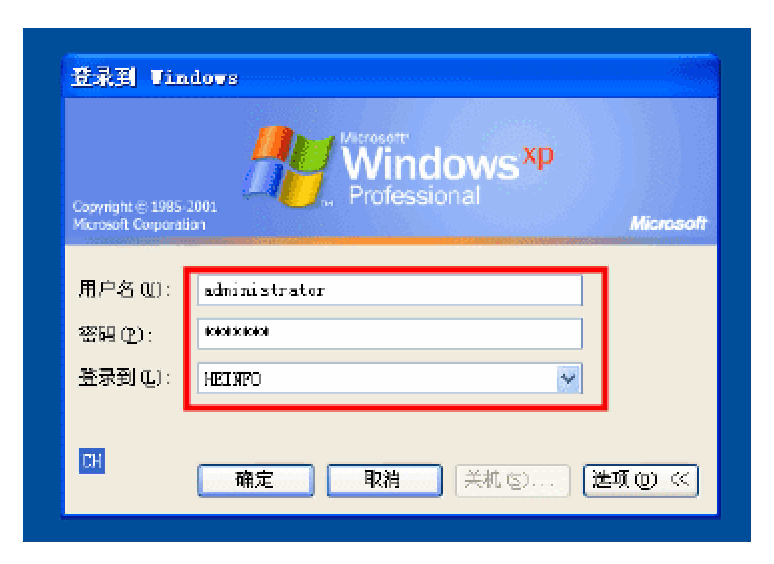


图 7-41　以域管理员账户登录

7.5.2　将用户添加到本地管理员组

默认情况下，普通域用户不能在其所登录的计算机上安装软件。不过，只要将计算机使用者的“域用户名”添加到当前计算机的“本地管理员组”就可以了。通常来说，将普通域用户添加到“本地管理员”组，有以下两种方法：

- 由管理员在服务器上打开“Active Directory 用户和计算机”窗口，从“Computer”组中选中用户的计算机，在快捷菜单中选择“管理”命令，打开工作站的“计算机管理”窗口，即可从“本地用户和组”中添加。
- 使用域管理员登录到工作站，打开“计算机管理”→“本地用户和组”进行添加。

这两种方法都需要使用者有域管理员权限，通常情况下由管理员进行操作。下面详细介绍这两种方法。

1. 在域服务器上添加

在 Windows Server 2008 服务器中，管理工作站，将域用户添加到工作站的“本地管理员组”的操作步骤如下。

01 在 Windows Server 2008 服务器中，以管理员身份登录，打开“服务器管理器”，在左侧任务窗格中定位到“角色→勾选 Directory 域服务→Active Directory 用户和计算机”，或者在“管理工具”中打开“Active Directory 用户和计算机”管理单元，都可以实现相同的功能。

在“Active Directory 用户和计算机”管理单元中，在左侧选择“Computers”，在右侧窗口列出所有加入域的计算机，选中要管理的计算机，使用鼠标右击，在弹出的快捷菜单中选择“管理”选项，如图 7-42 所示。

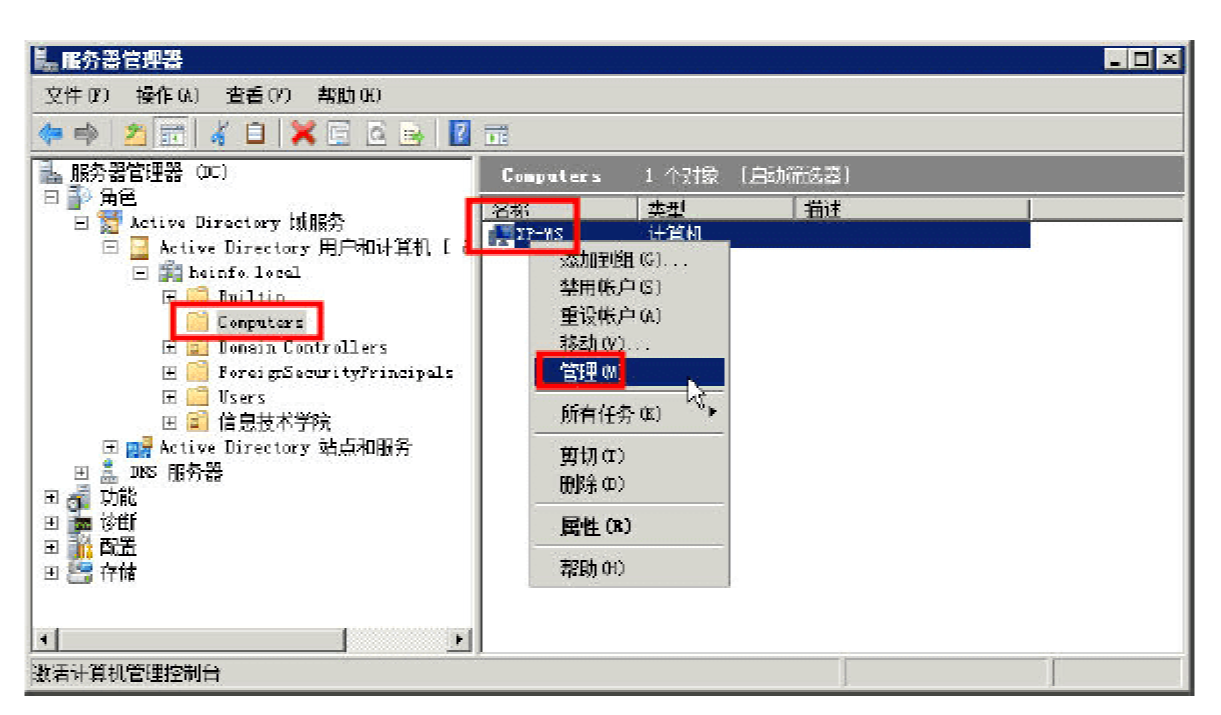


图 7-42　管理计算机

02 如果出现“无法管理计算机……”的提示（如图 7-43 所示），请切换到 Windows XP 的计算机，关闭 Windows XP 的防火墙设置（如图 7-44 所示），或者在“例外”选项卡中选中“文

件和打印共享”复选框即可。然后再返回到步骤 1 重新操作。

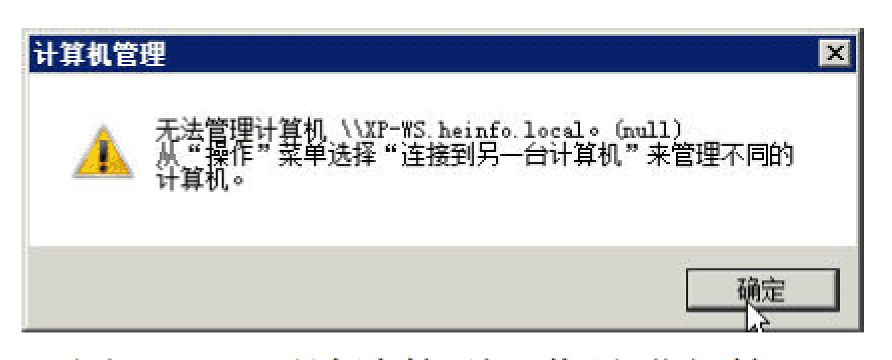


图 7-43　无法连接到工作站进行管理



图 7-44　关闭工作站的防火墙

03 重复步骤 1 之后，打开工作站的“计算机管理”对话框，定位到“本地用户和组→组”，在右侧用鼠标右击“Administrators”，在弹出的快捷菜单中选择“属性”选项，如图 7-45 所示。

04 打开“Administrators 属性”对话框，在“成员”列表中可以看到，当前管理员组中的账户分别是“HEINFO\Domain Admins”（这是 heinfo 域的管理员组）、“XP-WSAdministrator”（这是名为 XP-WS 计算机名的计算机中的本地管理员账户）、“XP-WS\LN”（这是 XP-WS 计算机的另一个本地管理员账户）。单击“添加”按钮，在弹出的“选择用户、计算机或组”对话框中，在“输入对象名称来选择”文本框中，输入要添加的域用户或域用户组，在此输入 domain users 表示域中所有用户），然后单击两次“确定”按钮，完成添加，如图 7-46 所示。

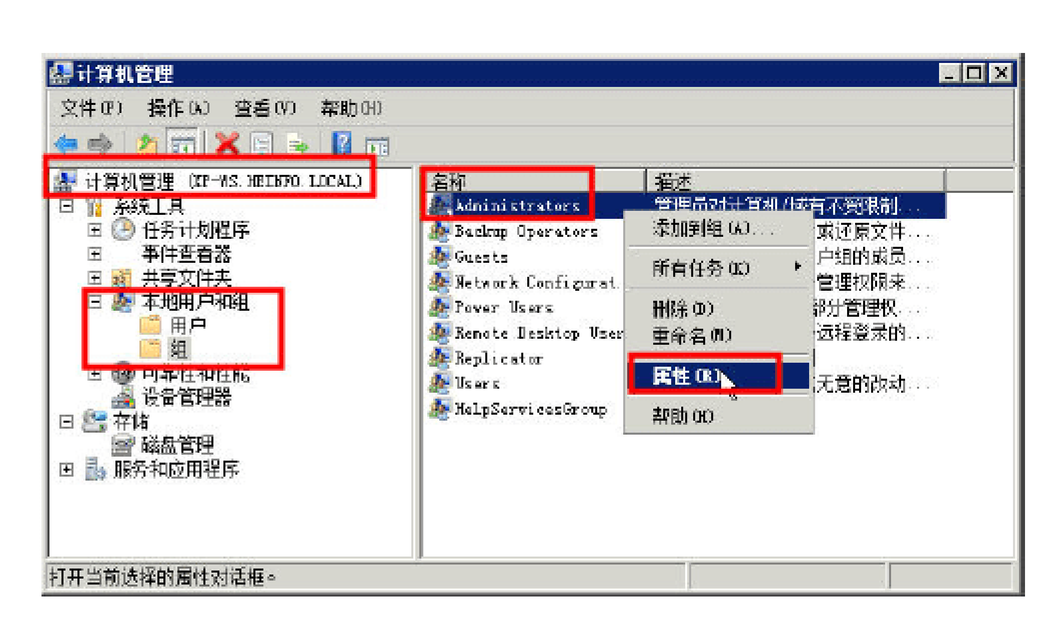


图 7-45　Administrators 组属性

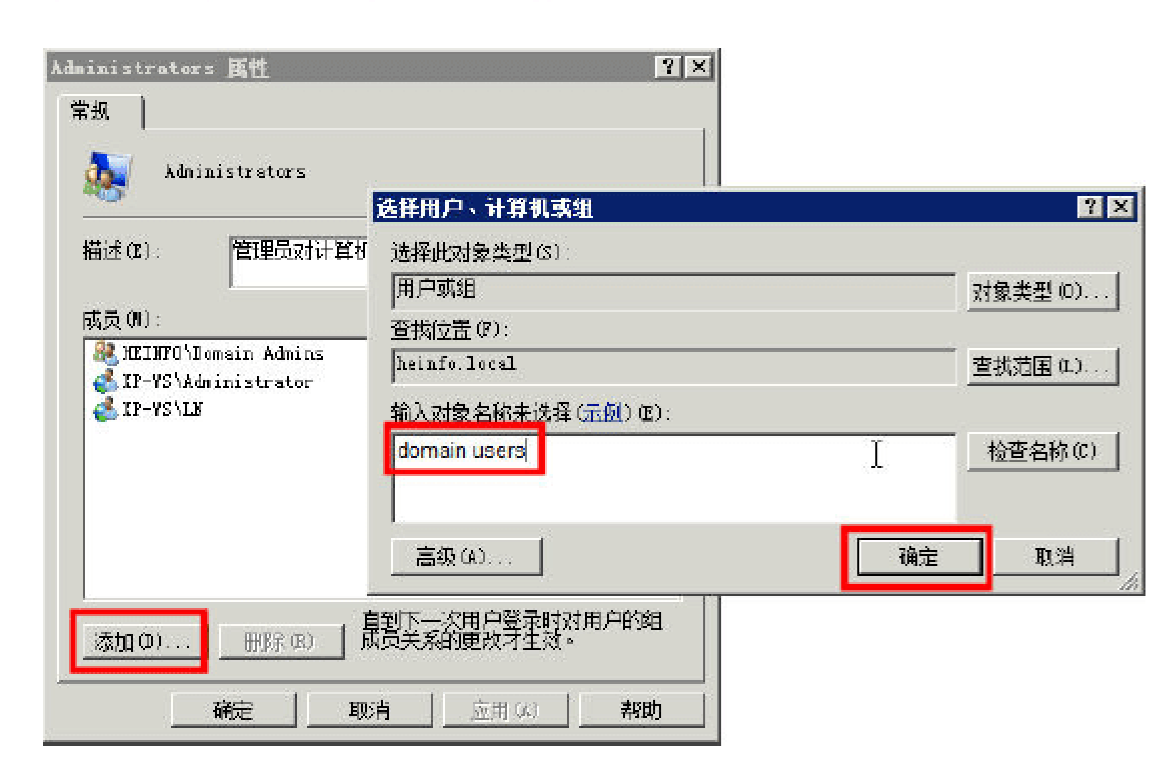


图 7-46　添加域用户组

说 明

在实际的网络管理中，应该在“本地管理员组”中，添加使用计算机的所有的域用户账户账户，而不是添加 Domain Users 域用户组。在做实验时，为了省事，可以这样做。

2. 在本地计算机上添加

对于计算机的使用者，他们在将自己的 Windows XP（或 Windows Vista、Windows 7）等工作站加入到域之后，可以使用自己的“本地管理员账户账户”登录，完成将“域用户账户或域用户账

户组”添加到“本地管理员组”的工作，主要步骤如下。

01 用管理员账户登录工作站，将计算机添加到 Active Directory 并重新启动。启动后使用“本地管理员账户”登录到本机。

02 用鼠标右键单击“我的电脑”，从快捷菜单中选择“管理”选项，显示“计算机管理”对话框。依次选择“系统工具→本地用户和组→组”，如图 7-47 所示。

03 在窗口右侧双击 Administrators 打开 “Administrators 属性”对话框，单击“添加”按钮，添加域用户账户，如图 7-48 所示。

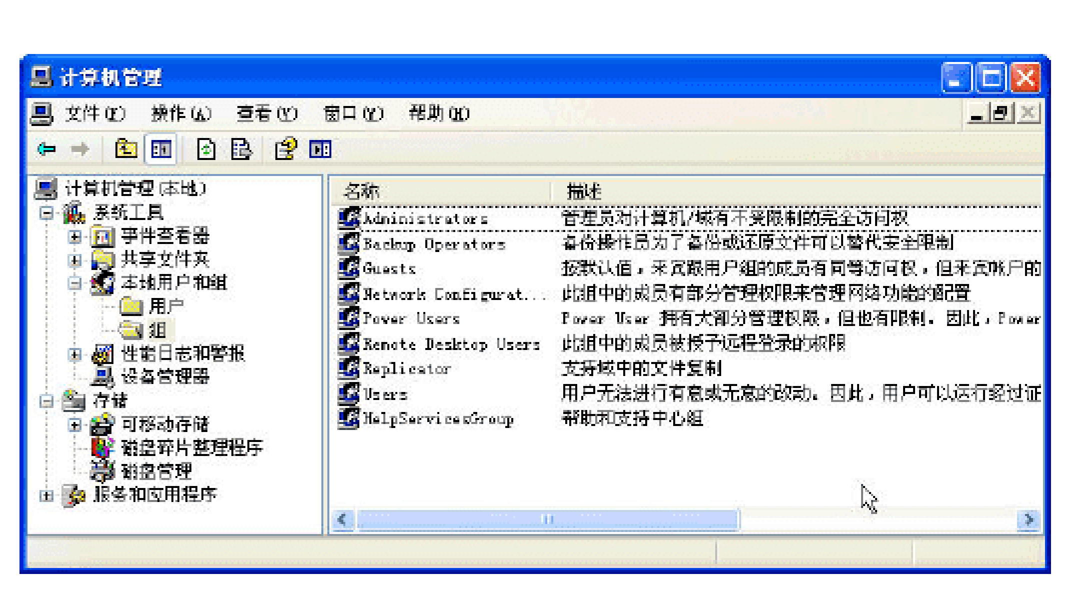


图 7-47　计算机管理对话框

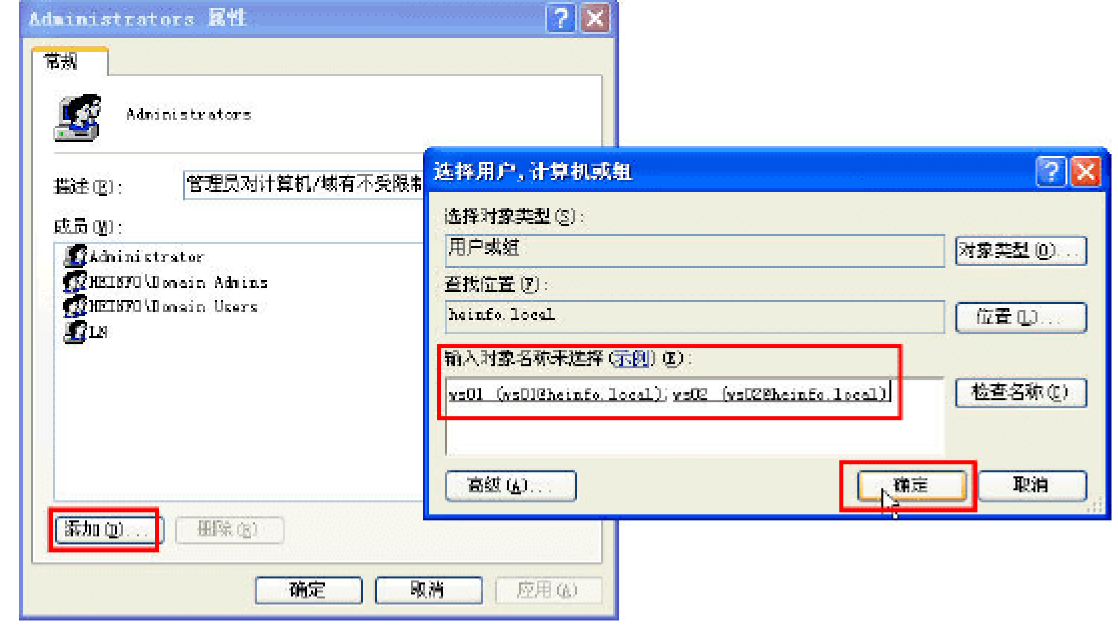


图 7-48　添加域用户账户

在实际的添加工作中，会弹出“输入用户名或密码”的提示，此时，输入自己的域用户账户及密码即可（由管理员分配）；如果是做实验，可以使用域管理员账户或密码，或者采用前面创建的名为 ws01 的用户名及密码。

04 单击“确定”按钮，将域用户加入管理员组成功。注销当前用户，并重新登录到域即可。

7.5.3　将 Windows 7 计算机添加到域

将 Windows 7 加入到域的步骤，与 Windows XP 类似，主要操作如下。

01 修改 Windows 7 的计算机名称，如图 7-49 所示。设置 IP 地址与 DNS，如图 7-50 所示。



图 7-49　修改计算机名称

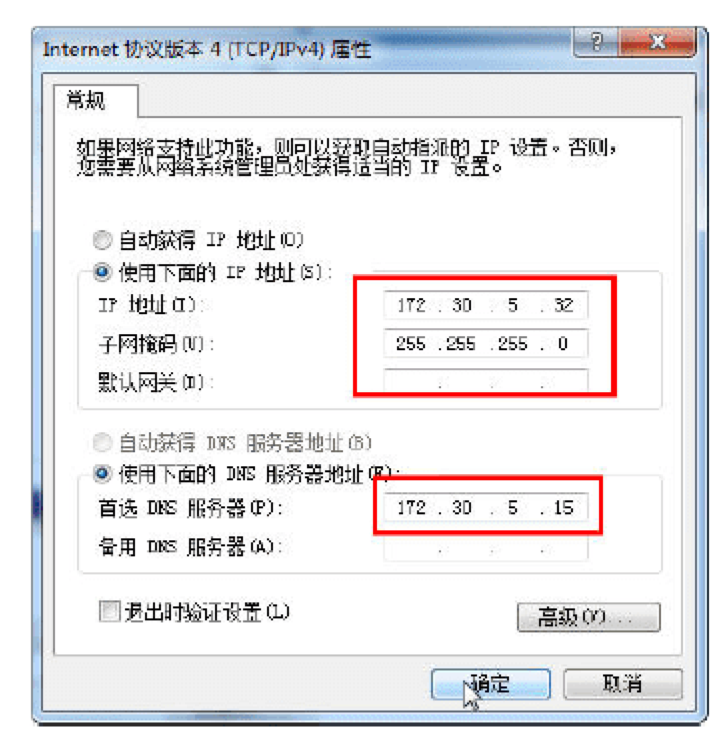


图 7-50　设置 IP 地址与 DNS

02 使用管理员账户登录，将计算机加入到 heinfo.local 域，在弹出“计算机名/域更改”对话框中，输入域管理员账户与密码，如图 7-51 所示。

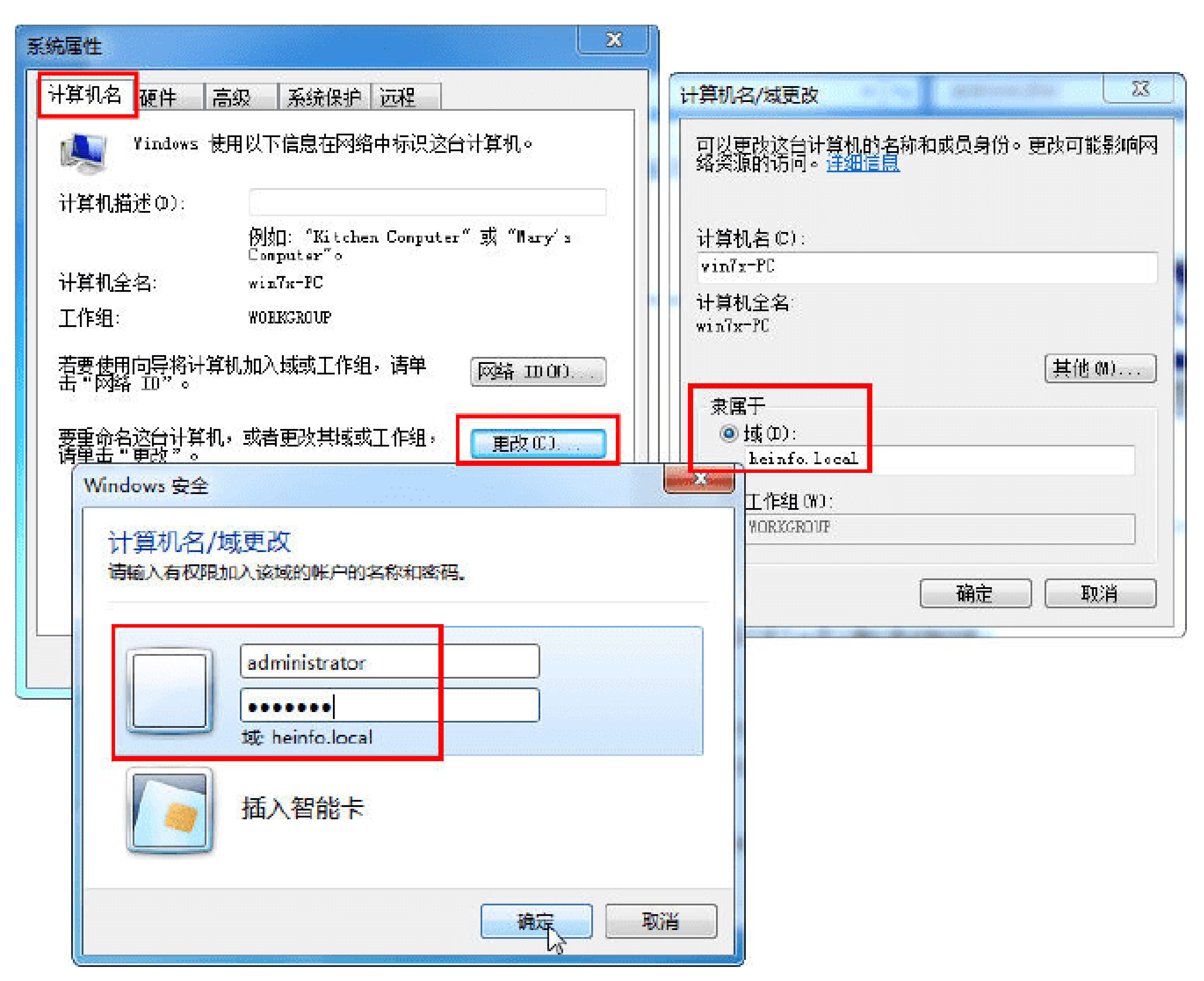


图 7-51　将计算机加入到域

03 在加入到域之后，先不要重新启动计算机，定位到“计算机管理→系统工具→本地用户和组→组”，在右侧窗格，用鼠标右击 Administrators，在弹出的对话框中选择“添加到组”选项，如图 7-52 所示。

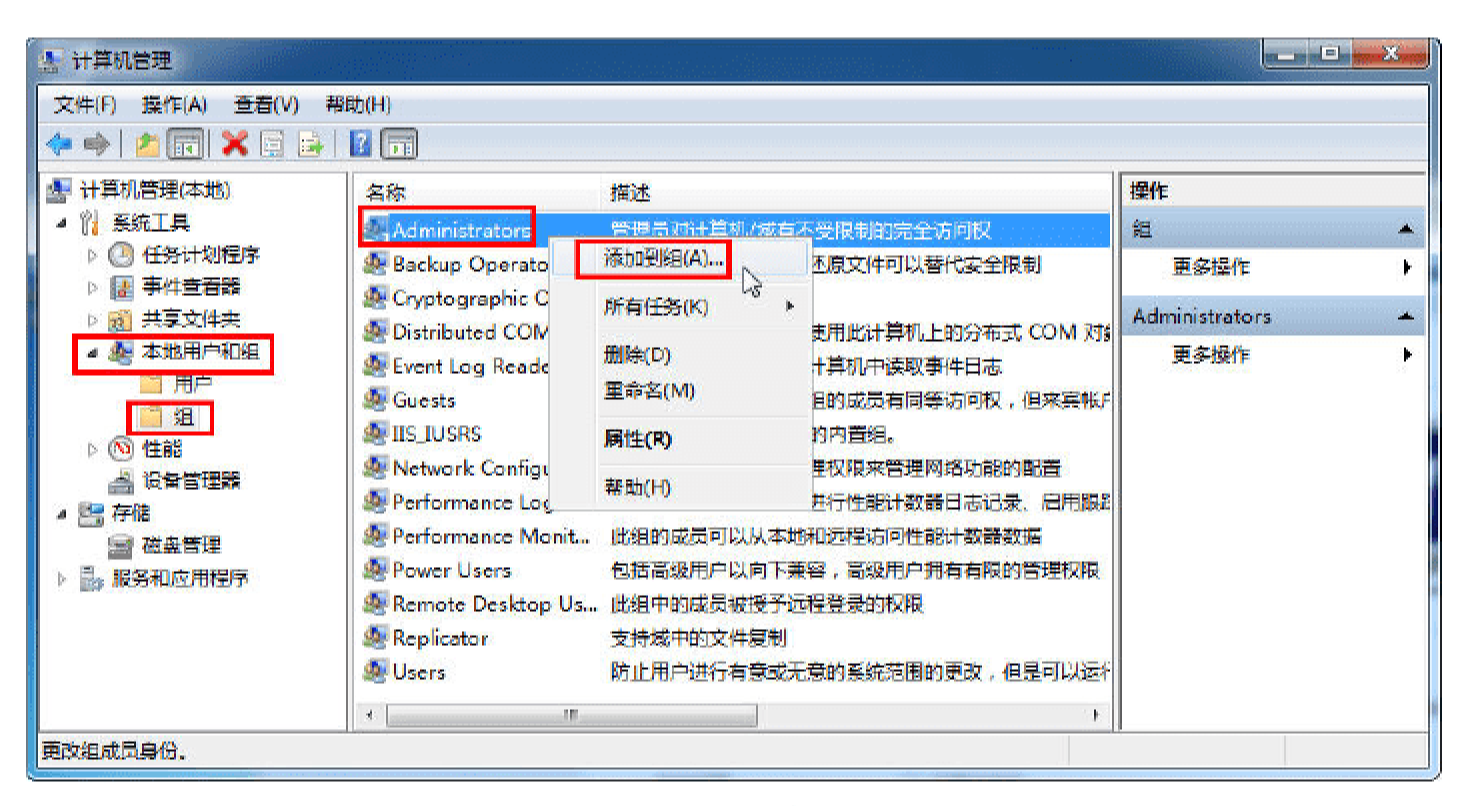


图 7-52　添加到组

04 在“Administrators 属性”对话框中，单击“添加”按钮，在弹出的“选择用户、计算机、服务账户或组”对话框中，在“输入对象名称来选择”文本框中，输入想要添加的域用户账户或组，单击“检查名称”按钮，此时会弹出“输入网络密码”对话框，输入域用户账户（例如前面章节中创建的 ws01 账户），然后单击“确定”按钮，如图 7-53 所示。

05 添加之后，关闭“计算机管理”窗口，然后重新启动 Windows 7，完成将计算机加入到域、将域用户添加到本地管理员组的操作。

图 7-53　添加 Domain Users 组到 Administrators 组

7.6　使用远程管理工具管理 Active Directory 服务器

在实际的网络中，Windows Server 2008 服务器会放在机房中，对于管理员来说，需要经常登录服务器进行管理，例如创建账户、修改共享文件夹、使用服务器的其他服务（例如管理 WSUS、管理证书服务、管理 IIS 等）。对于管理员来说，不可能每次都去机房、到服务器前去执行管理操作。通常来说，管理员管理 Windows 服务器有两种方法：

（1）使用远程桌面管理工具，例如使用“远程桌面”或其他远程管理工具，例如 TeamView、WinVNC 等。

（2）使用远程管理工具。在 Windows Server 2003 的时代，通常采用 Active Directory 管理工具+MMC 管理控制台的方式。而在 Windows Server 2008 的时代，通常使用“远程管理工具”管理服务器。

使用“远程桌面”，只要在“服务器”一端启用“远程桌面”或安装终端服务器，在工作站使用“远程桌面”就可以连接并登录到服务器进行管理。如果使用“远程管理工具”，需要在加入到域的 Windows Vista、Windows 7、Windows Server 2008、Windows Server 2008 R2 中，添加“远程服务器管理工具”才能使用。

7.6.1　添加远程服务器管理工具

如果工作站是 Windows Server 2008、Windows Server 2008 R2 的操作系统，可以在“服务器管理器”中，通过“功能→添加功能”命令，在“选择功能”对话框中，在“远程服务器管理工具”中，选择并添加要安装的服务器管理工具，例如 Web 服务器（IIS）管理工具、Active Directory 管理工具、DHCP 服务器管理工具、DNS 服务器管理工具、Hyper-V 工具等，如图 7-54 所示。

添加之后，就可以打开“服务器管理器”，使用相应的服务器管理工具管理远程的服务器了。



图 7-54　添加远程服务器管理工具

7.6.2　在 Windows 7 中安装远程服务器管理工具

在 Windows 7 、Windows 7 SP1 中，没有集成“远程服务器管理工具”，需要从以下地址 http://www.microsoft.com/downloads/zh-cn/details.aspx?displaylang=zh-cn&FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d 下载用于 Windows 7 SP1 的远程服务器管理工具。下载之后，登录到 Windows 7，安装该工具，然后再次添加，主要步骤如下。

01 在域用户登录 Windows 7，如图 7-55 所示。

02 运行下载的 Windows 7 SP1 远程服务器管理工具，如图 7-56 所示。



图 7-55　以域用户登录

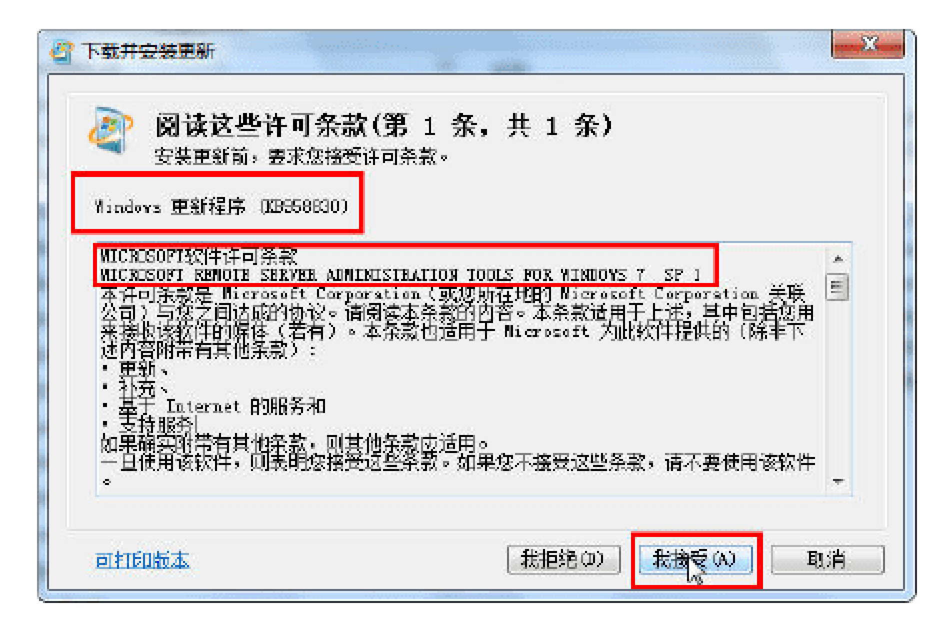


图 7-56　安装远程服务器管理工具



说 明

Windows 7 远程服务器管理工具仅可以安装在运行 Windows 7 企业版、专业版或旗舰版的操作系统上。

03 安装完成之后，从“控制面板”中运行“程序和功能”，单击“打开或关闭 Windows 功能”链接，如图 7-57 所示。

04 在“打开或关闭 Windows 功能”对话框，在“远程服务器管理工具”中，根据需要选择安装，或者安装全部的功能，如图 7-58 所示。

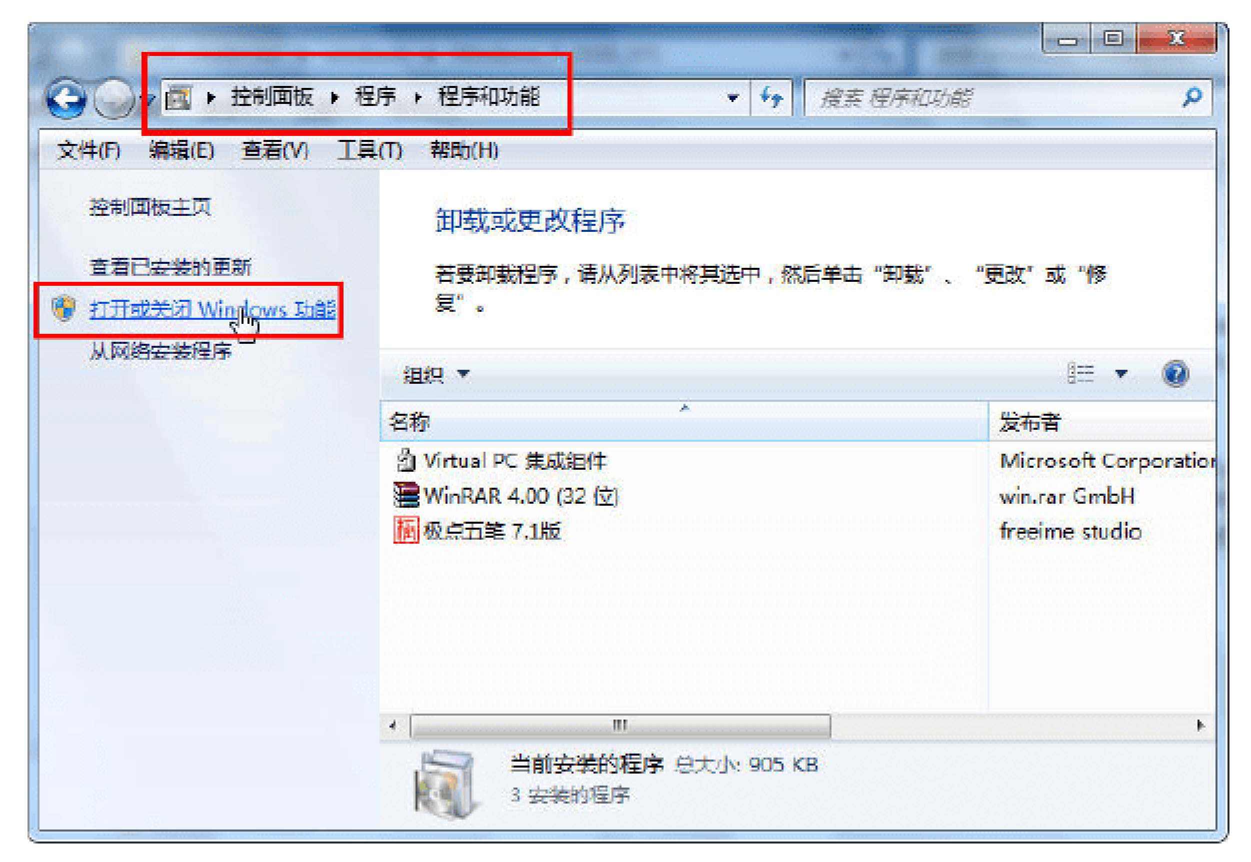


图 7-57　打开或关闭 Windows 功能

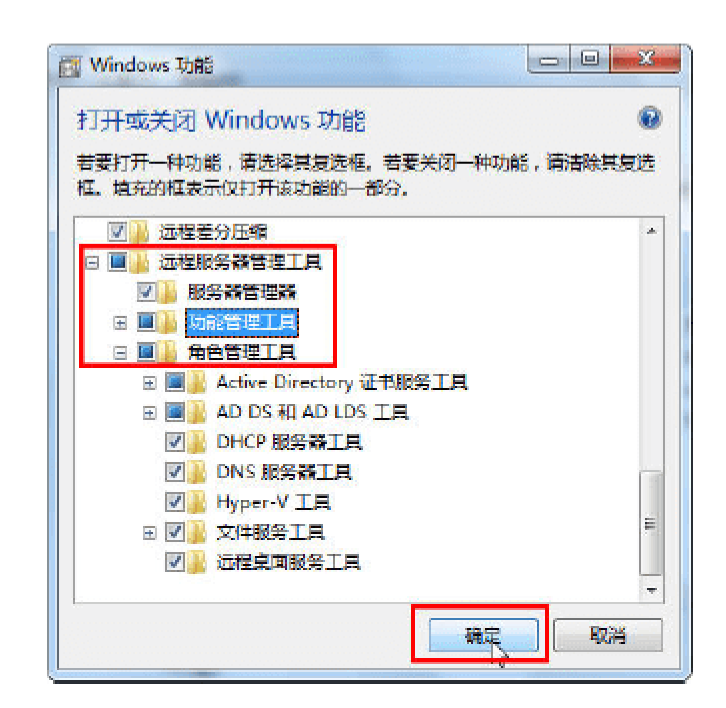


图 7-58　安装远程服务器管理工具

安装完成之后，就可以使用远程管理工具管理 Active Directory 服务器了。

第 8 章　使用组策略管理网络

组策略（Group Policy）是 Windows 2000 Server、Windows Server 2003、Windows Server2008、Windows Server 2008 R2 域网络的重要内容，可以对 Active Directory 中的工作站、服务器进行集中和统一的管理。使用组策略可以完成终端界面（用户环境）定制、终端软件定制、软件自动分发与自动安装等一系列工作，可以极大的减少网络管理员与使用者的操作步骤，减轻网络管理员和用户的负担。

8.1 组策略应用基础

“组策略”是 Microsoft 从 Windows 2000 Server 开始提供的功能，并在 Windows Server 2008 R2 中继续应用与推广。使用“组策略”，可以管理 Microsoft Windows Server 2008 与 Windows Server 2008 R2 家族中包括的高级功能，如软件安装、管理模板、文件夹重定向、远程安装服务、安全设置、脚本（启动/关机和登录/注销）以及 Internet Explorer 维护。

8.1.1 组策略概述

“组策略”可以完成用户所需要的软件自动安装、自动定制用户环境、自动将用户的文件夹重定向到服务器等一系列高级功能，而无须管理员和用户单独设置。功能详细介绍如下：

（1）完成客户端软件的自动安装。在一个企业网络中，通常每个部门使用的软件是不尽相同的。在以前（如 NT）的网络中，这只能由网络管理员给每一台计算机按照不同的用户需求安装软件。在应用组策略后，每个用户需要的软件在第一次使用时自动安装，用户只须做极少的设置或无须设置即可完成。

（2）将用户的习惯设置与数据“自动”带到另一台计算机。例如，用户 A 先在计算机 A 上工作，然后由于工作需求，用户 A 在计算机 A 上注销之后，马上就到了计算机 B 上进行工作，此时用户 A 的数据与习惯设置将会“自动”带到计算机 B 上。

（3）应用程序跟随用户。例如，用户 A 使用 Office 2003，在用户 A 的计算机上安装的 Office 2003；用户 B 使用 WPS Office 2003，在用户 B 的计算机上安装的就是 WPS Office 2003。如果用户 A 使用他的用户名在用户 B 的计算机上登录后，当用户 A 使用 Office 2003 或者双击 Office System 2003 的数据文档，就会在计算机 B 上安装 Office 2003，这一切都是自动进行的。

（4）为用户定制统一的工作环境。当第一次使用加入到域的 Windows 操作系统（例如 Windows XP、Windows 7、Windows 2003、Windows Server 2008、Windows Server 2008 R2）时，用户都要

对系统做一些设置，如设置 IE、设置桌面等，而这一切都可以由组策略来定制。

（5）灾难恢复更加容易。如果用户使用的计算机突然损坏，如硬盘损坏。此时，只要换一块新硬盘到原来的计算机中，或者把坏计算机替换，重新安装一台全新的计算机即可。用户仅仅是按照系统管理员的提示按下计算机键盘上的一个键，或者用一张特定的软盘启动计算机，用户所需要的操作系统、应用程序及用户的数据、习惯设置都会自动恢复。

总之，应用组策略将极大地减轻管理员和用户的负担，同时为用户提供了更高的安全性及更好的便利性。

8.1.2　委派用户权限

想要实现组策略，网络中的工作站（Windows 2000 Professional、Windows XP Professional、Windows 7）必须添加到 Active Directory 域中，而且只有管理员或管理员委派的用户才有权将计算机加入到域中。如果网络管理员将计算机一个一个添加到域中，则比较麻烦，通常的做法是委派域用户组，让所有的域用户具有“将计算机加入到域”的操作，这样，对于每个用户来说，他可以自己完成将计算机加入到域、然后将自己的域用户添加到“本地管理员组”的操作。要想实现这个功能，需要委派“Domain Users”组具有将计算机加入到域的权限，主要步骤如下。

01 在“服务器管理器”中定位到“角色→Active Directory 域服务→Active Directory 用户和计算机”，或者从“管理工具”中运行“Active Directory 用户和计算机”，右击域名 heinfo.local，从快捷菜单中选择“委派控制”选项，如图 8-1 所示，启动“控制委派向导”。

02 在“用户或组”对话框，单击“添加”按钮，显示“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中输入将要委派的用户或用户组名，在本例中输入 Domain Users，然后单击“检查名称”按钮，随后单击“确定”按钮，如图 8-2 所示。

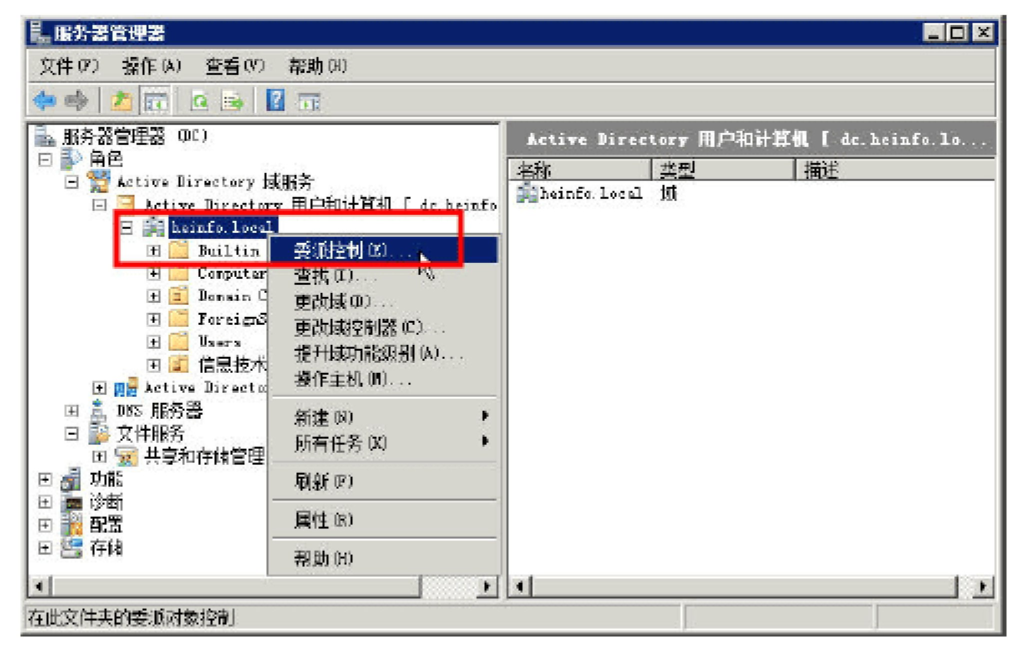
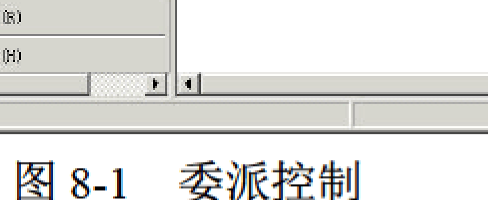



图 8-1　委派控制

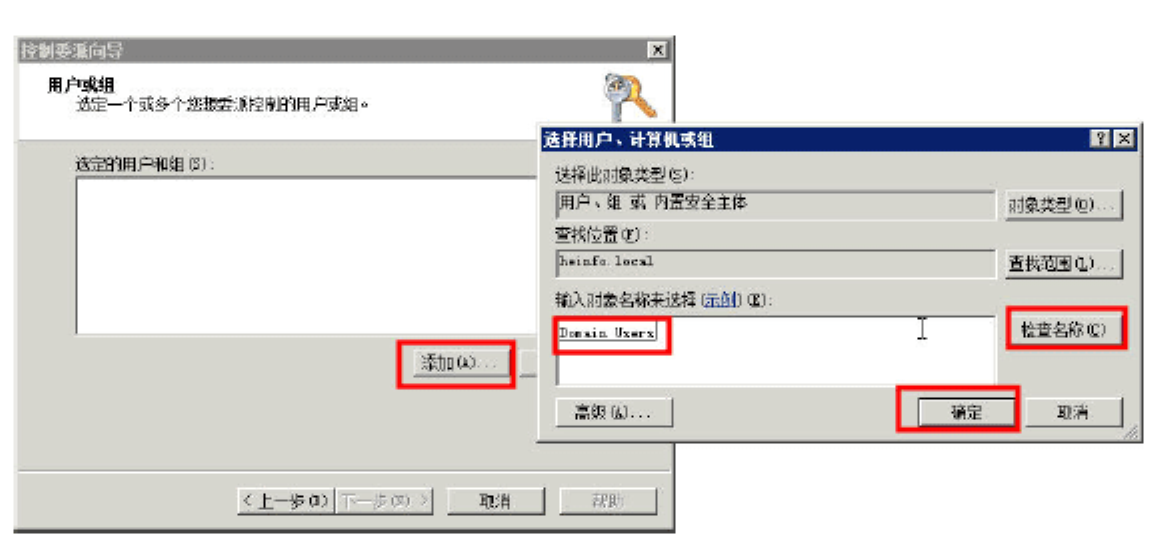


图 8-2　添加委派用户和用户组

03 在“要委派的任务”对话框中，选中“将计算机加入到域”选项，如图 8-3 所示。

04 在“完成控制委派向导”对话框，显示了委派的任务，单击“完成”按钮，如图 8-4 所示，完成委派。

经过上述操作之后，每个域用户都具有了“将计算机加入到域”的权限。

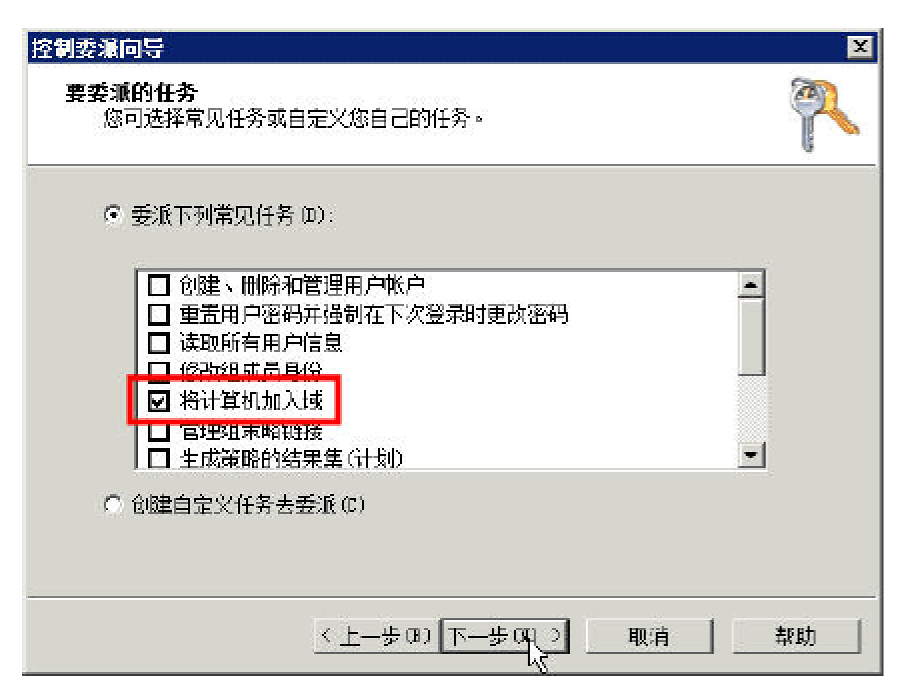




图 8-3　委派“将计算机加入到域”权限

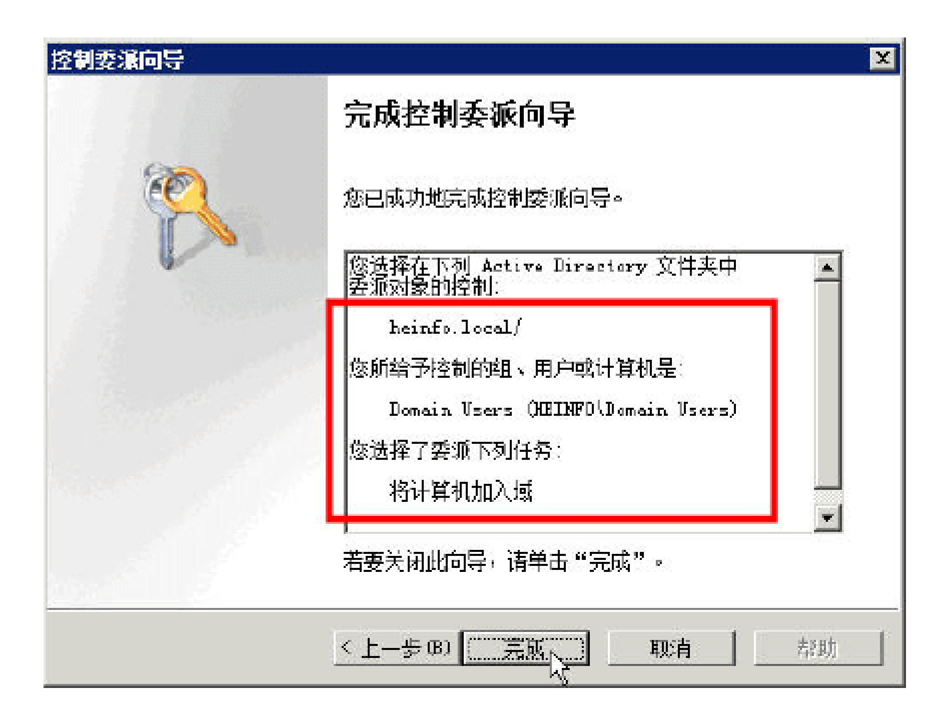


图 8-4　完成委派任务

我们知道，在 Active Directory 网络中，Administrator 及加入到 Administrators、Domain Admins 组的用户，具有管理员权限，可以添加、删除用户、修改用户密码、管理共享等。在实际的企业网络中，尤其是在大型的企业网络中，可能用户量很大、部门也很多，这个时候，域管理员可以将一部分权限，例如创建用户、修改用户密码等，委派给每个部门中的“部门管理员”。这样可以减轻域管理员的负担，并且可以提高管理的效率（添加用户、修改密码等问题可以直接找自己的“部门管理员”）。

在下面的内容中，在“信息技术学院”组织单位中，创建一个名为 heinfo-admin 的用户，并且使用“委派权限”的方法，委派 heinfo-admin 具有在“信息技术学院”组织单位中创建用户、修改密码等权限（该权限限制于指定的组织单位中），操作步骤如下。

01 在“heinfo.local\信息技术学院”组织单位中创建 heinfo-admin 用户，如图 8-5 所示。

02 右击“信息技术学院”组织单位，在弹出的快捷菜单中选择“委派控制”选项，如图 8-6 所示。



图 8-5　创建用户

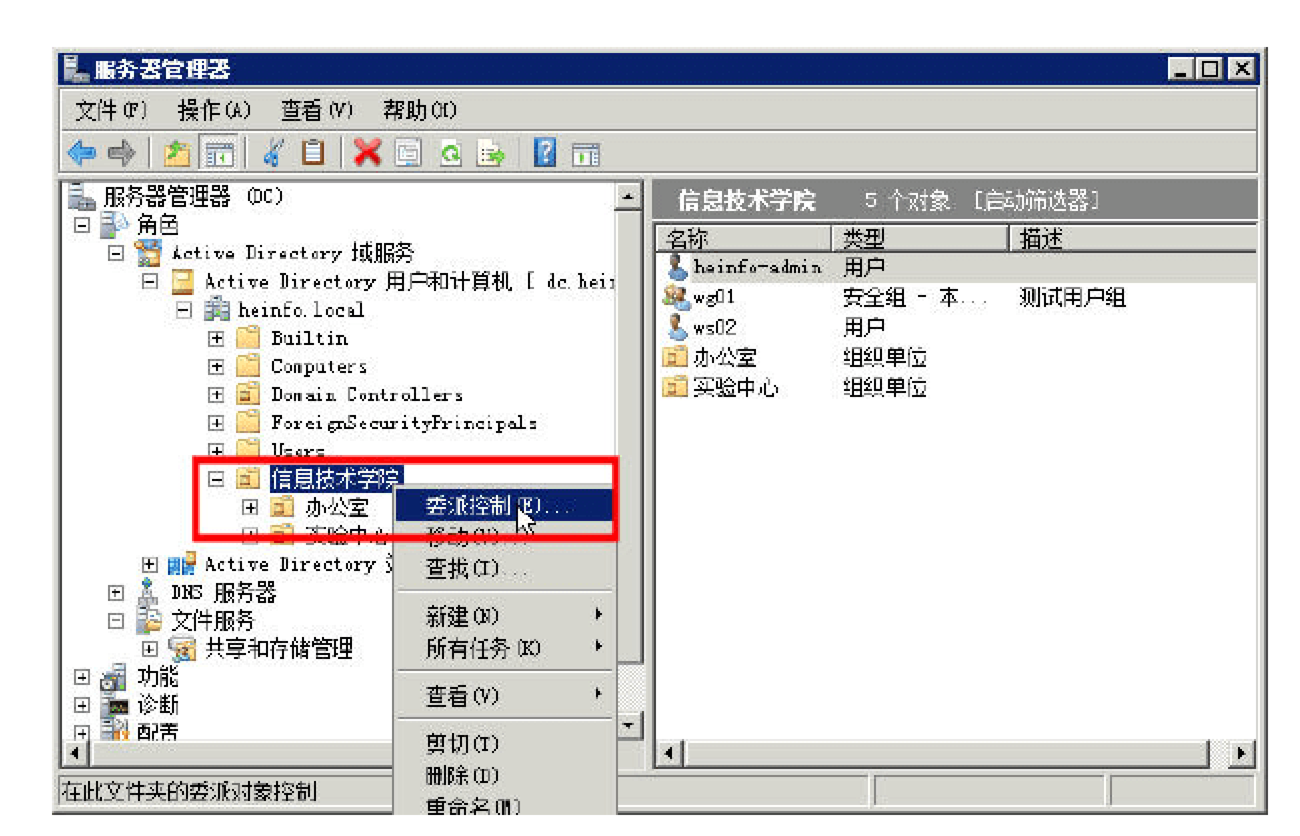


图 8-6　在指定 OU 中进行委派控制

03 在“用户或组”对话框中，单击“heinfo-admin”用户，如图 8-7 所示。

04 在“要委派的任务”对话框中，根据需要运行选择，在此选中前 6 项，如图 8-8 所示。

05 在“完成控制委派向导”对话框中，单击“完成”按钮，完成委派任务。

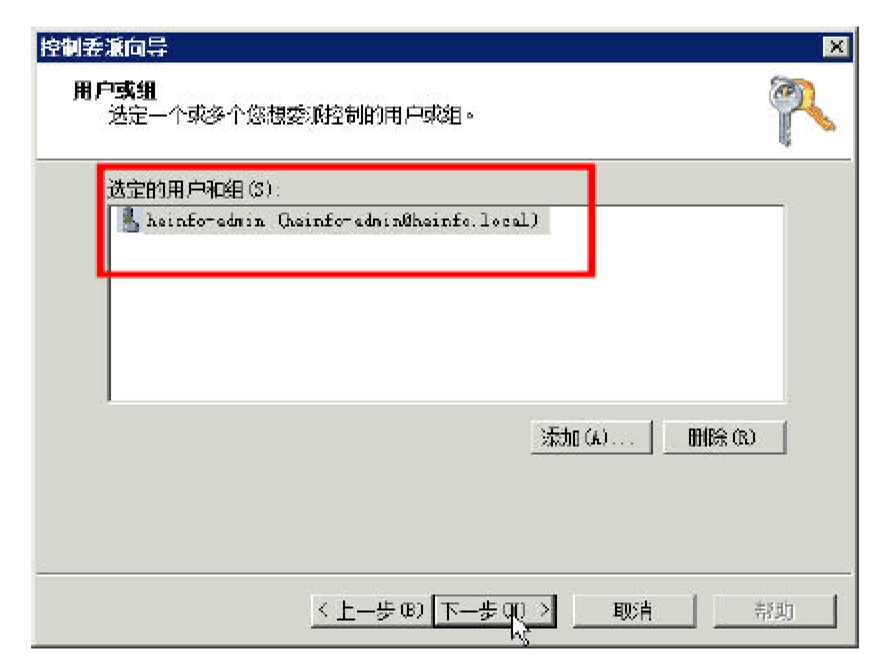


图 8-7 添加用户

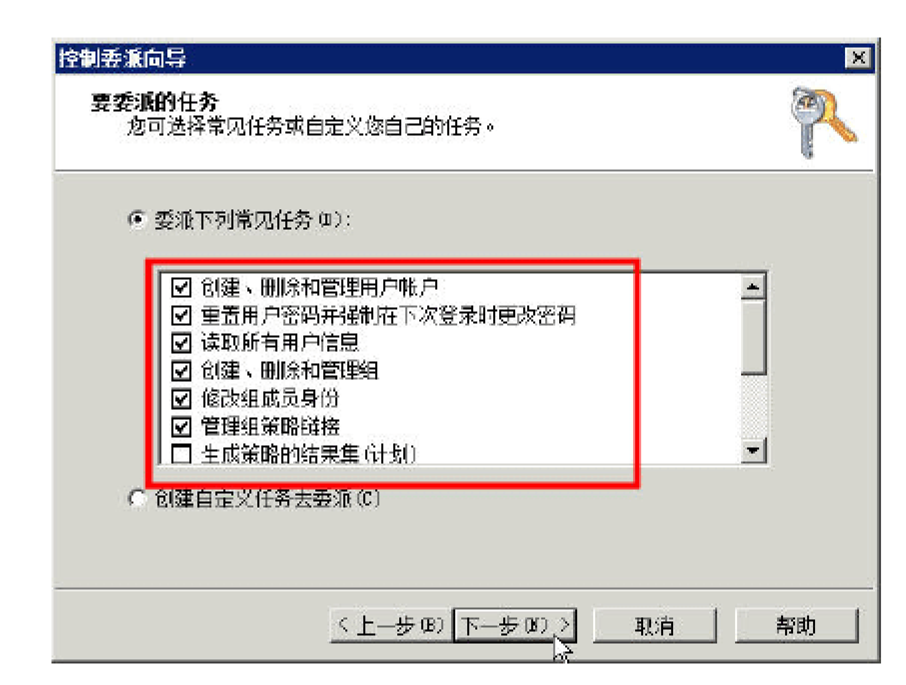


图 8-8 选择要委派的任务

以后当 heinfo-admin 登录后，或者在 Windows 7 的工作站上安装“远程服务器管理工具”，使用“服务器管理器”打开“Active Directory 用户和计算机”管理单元，就可以在“信息技术学院”组织单位中创建用户、删除用户、修改密码等操作。

在前面的操作中，我们委派了 Domain Users 与 heinfo-admin 用户，如果要删除这个操作，可以按照如下的步骤进行（以删除 heinfo-admin 的委派权限为例）。

01 在“Active Directory 用户和计算机”中，在“查看”菜单选择“高级功能”菜单命令，如图 8-9 所示。

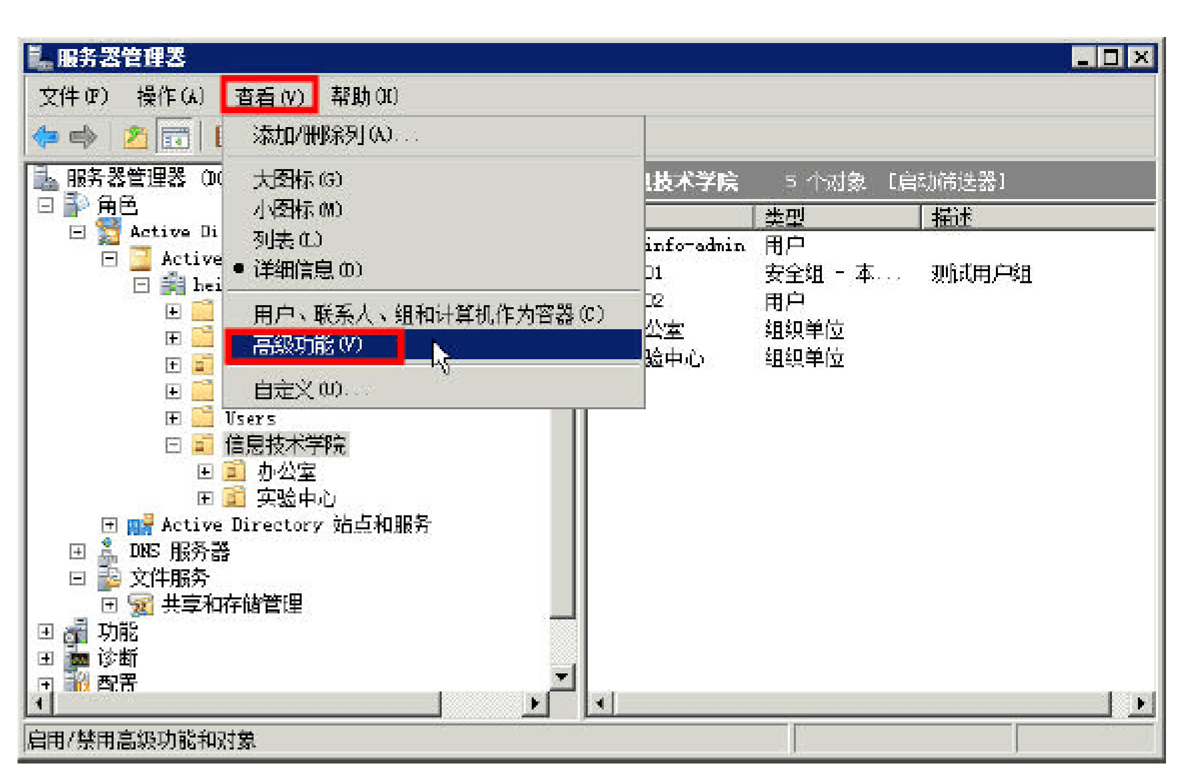
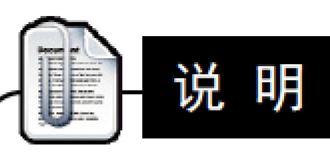


图 8-9 高级功能

02 右击“信息技术学院”组织单位，在弹出的快捷菜单中选择“属性”选项，如图 8-10 所示。

03 在“信息技术学院 属性”对话框中，在“安全”选项卡中，选中“heinfo-admin”选项，单击“删除”按钮，如图 8-11 所示，然后单击“确定”按钮就可以删除委派的 heinfo-admin 权限。



说 明

由于 Domain Users 权限是在“heinfo.local”中进行委派，所以，如果要删除该权限，需要右击“heinfo.local”并选择属性，打开 heinfo.local 的属性→安全选项卡，从列表中找到 Donain Users 组进行删除。

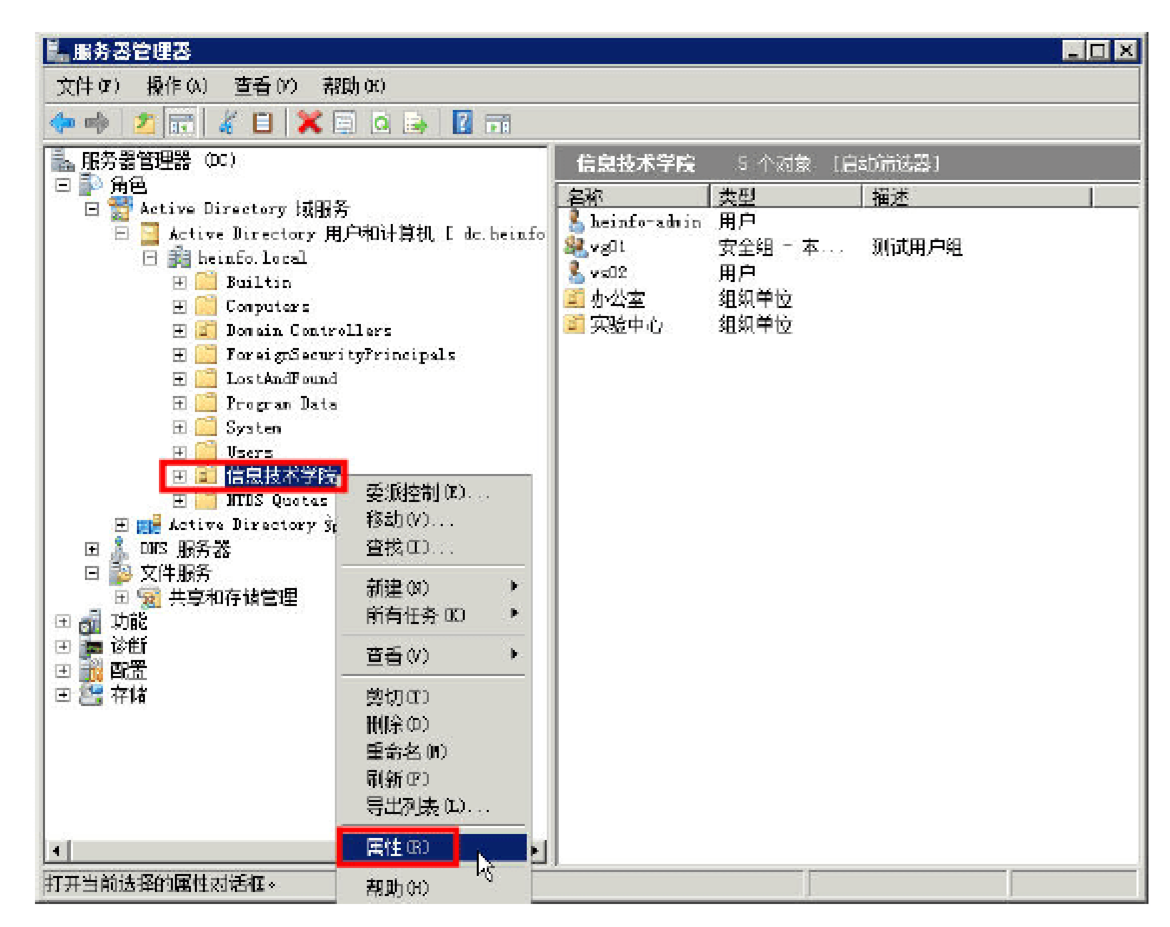



图 8-10　属性

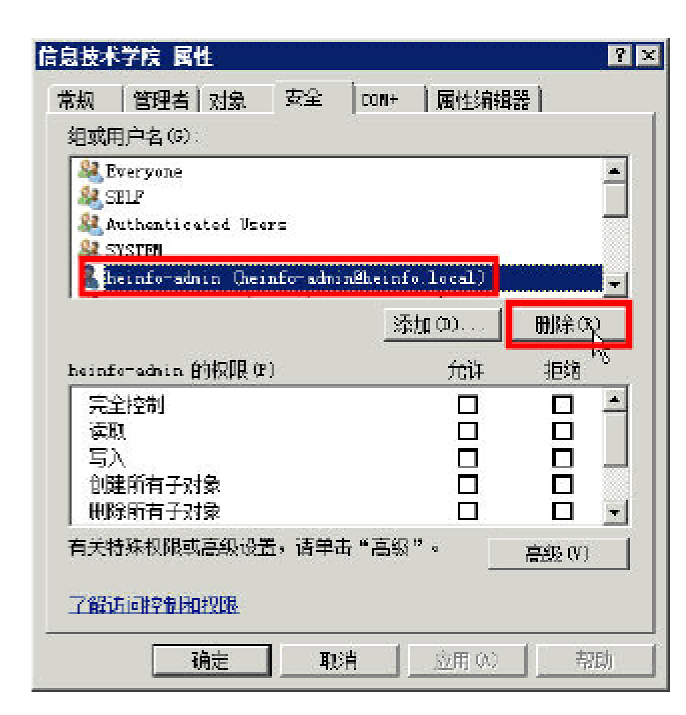


图 8-11　删除委派用户

8.1.3　默认组策略

组策略必须应用在组织单位上，子组织单位默认继承上一级组织单位的组策略。所以，通常将公共的任务设置在最上级的组织单位上，将专用的任务设置在具体应用的组织单位上。默认情况下，每个组织单位都继承使用上一级的组策略。在 Windows Server 2008 中，在“服务器管理器→功能→组策略管理”中，按照 Active Directory 的架构，管理组策略，如图 8-12 所示。

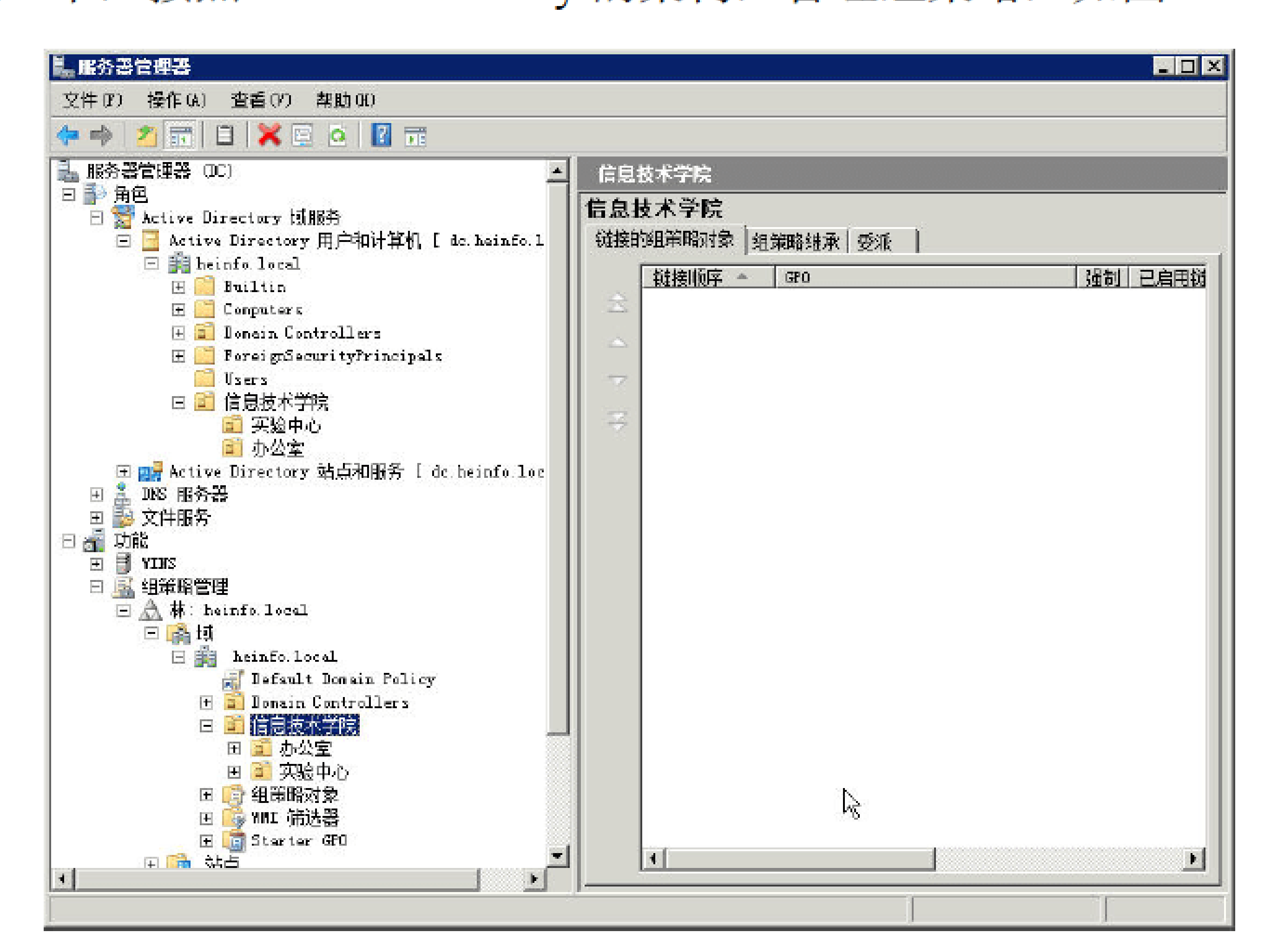


图 8-12　组策略管理

在图 8-12 中，在“角色→Active Directory 域服务→Active Directory 用户和计算机”中创建的“组织单位”及用户、用户组，在“功能→组策略管理”管理单元中，按照 Active Directory 的架构，显示对应的组织单位，并且在该管理单元中进行组策略的创建、删除与编辑。

首先看一下默认的策略。在“组策略管理”中，展开“Domain Controllers”，可以看到“Default Domain Controllers Policy”，这是默认的域控制器的策略，该策略只应用于 Active Directory 中的“域控制器”。而“heinfo.local”下面的“Default Domain Policy”将应用于域中的所有计算机（包括域

控制器）和用户。

当选中某条策略时，例如“Default Domain Controllers Policy”，在右侧的窗格中，会显示“作用域”、“详细信息”、“设置”、“委派”4 个选项卡，如图 8-13 所示。

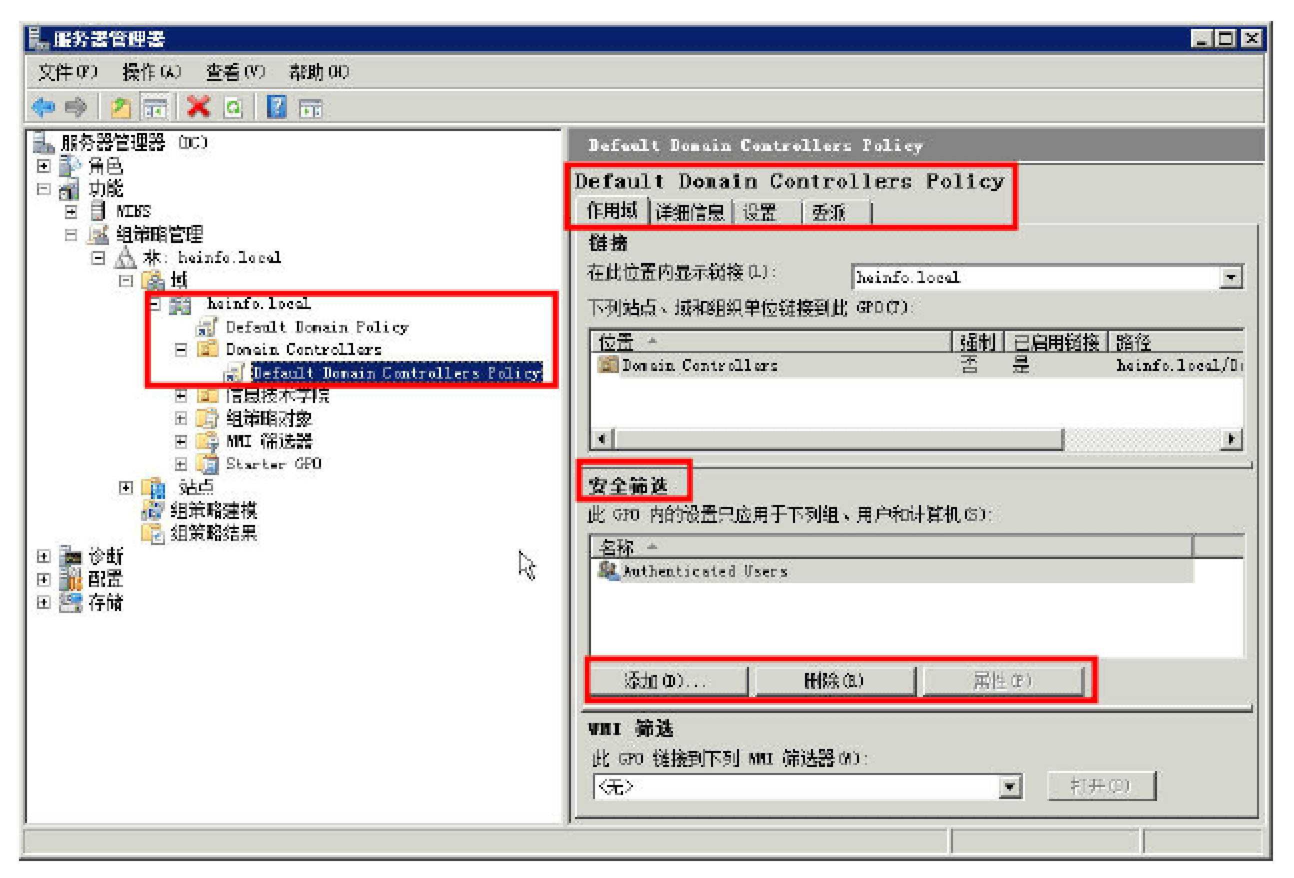
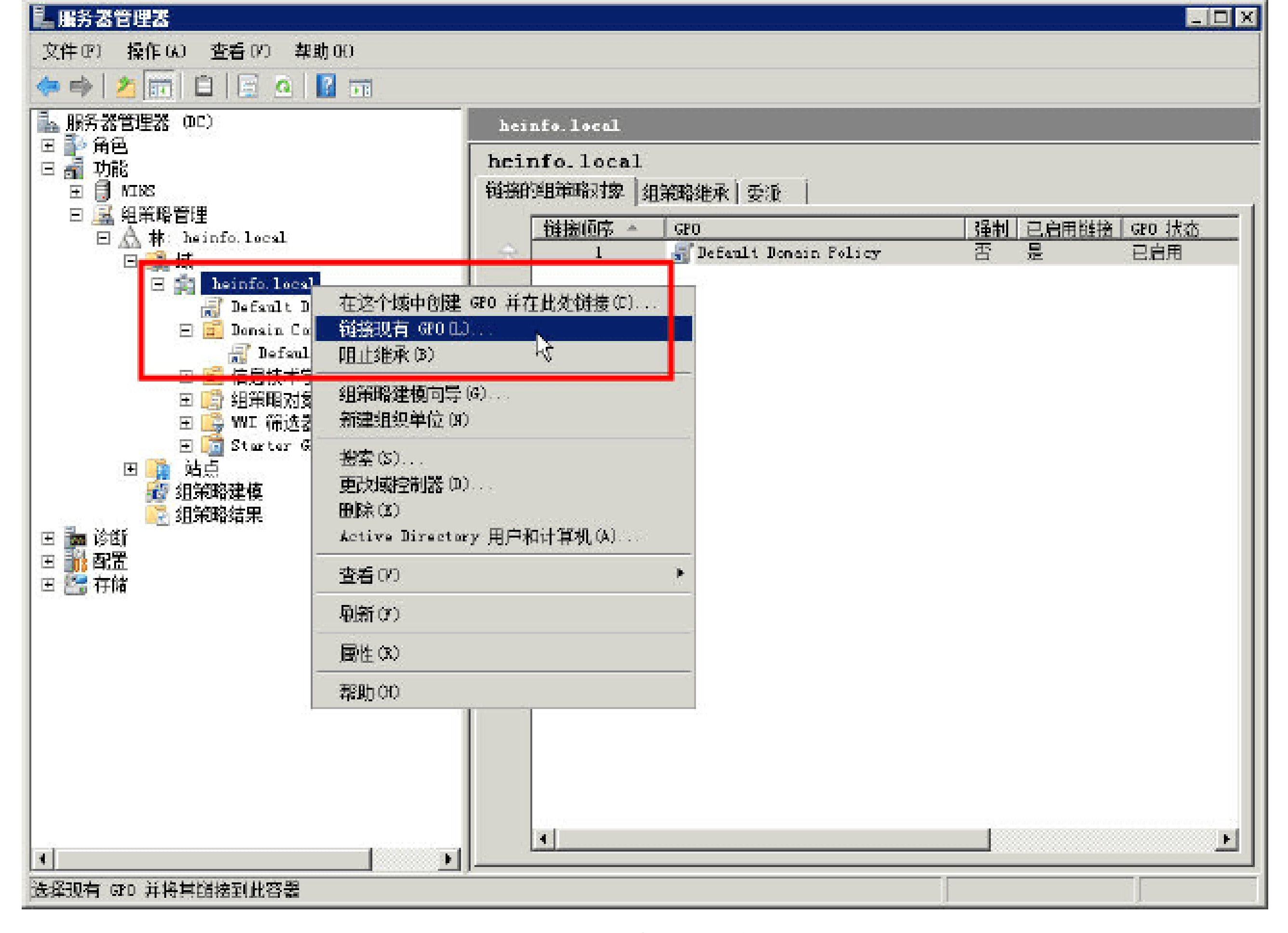


图 8-13　默认域控制器策略

在“作用域”选项卡中，显示了“链接”、“安全筛选”与“WMI 筛选”，其中“安全筛选”列表中，显示了当前 GPO（Group Policy Object，组策略对象）应用的目标组、用户和计算机，其中默认的“Authenticated Users”为“授权的组”，表示所有已经经过 Active Directory 授权的用户（即所有 Active Directory 用户）。如果你的组策略只用于指定的用户，可以删除“Authenticated Users”并添加指定的用户、用户组或计算机。在“链接”列表中，显示了当前组策略链接、是否强制、是否启用链接及路径，可以用鼠标右击列表中的链接，在弹出的快捷菜单中选择“强制”、“是否启用链接”、以及删除该策略（不要删除默认的域策略、默认的域控制器策略，可以删除自建的域策略），如果删除了默认的域策略，可以右击“heinfo.local”在弹出的快捷菜单中选择“链接现有 GPO”（如图 8-14 所示），在弹出的“选择 GPO”对话框中，选择“Default Domain Policy”，或者选择其他删除的 GPO，如图 8-15 所示。



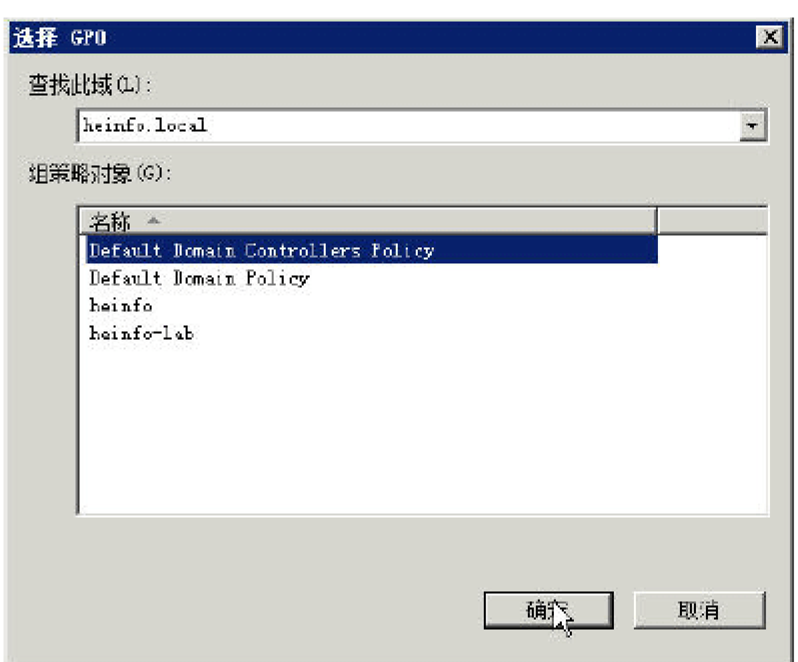


图 8-14　链接现有 GPO　　　　图 8-15　选择 GPO

在“详细信息”选项卡中，显示了 GPO 的状态，默认为“已启用”，如图 8-16 所示。

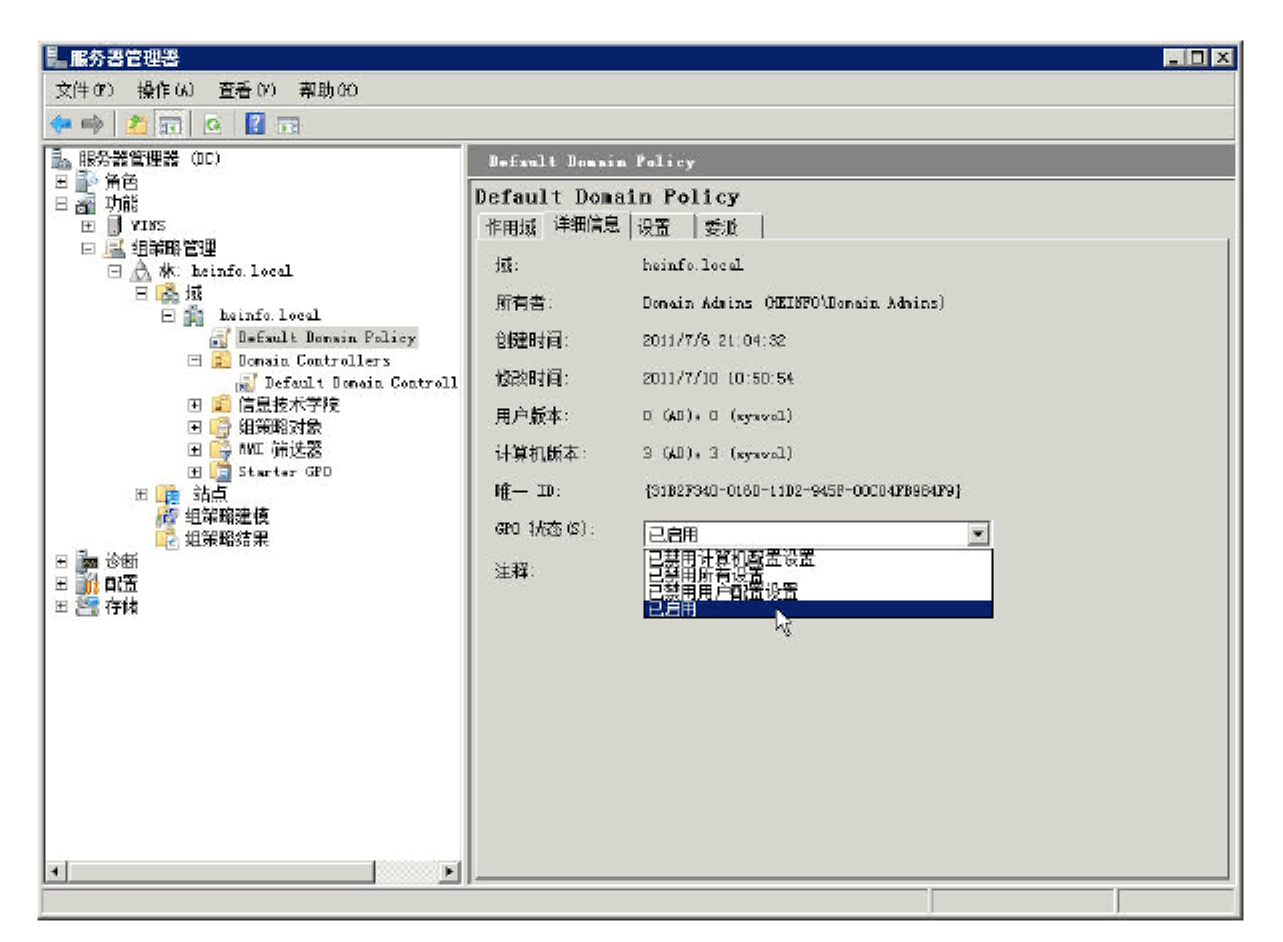


图 8-16　详细信息

在“设置”选项卡，显示了前选中的组策略的设置信息，如图 8-17 所示。可以单击“显示”或“隐藏”链接选择显示或隐藏每一项设置。

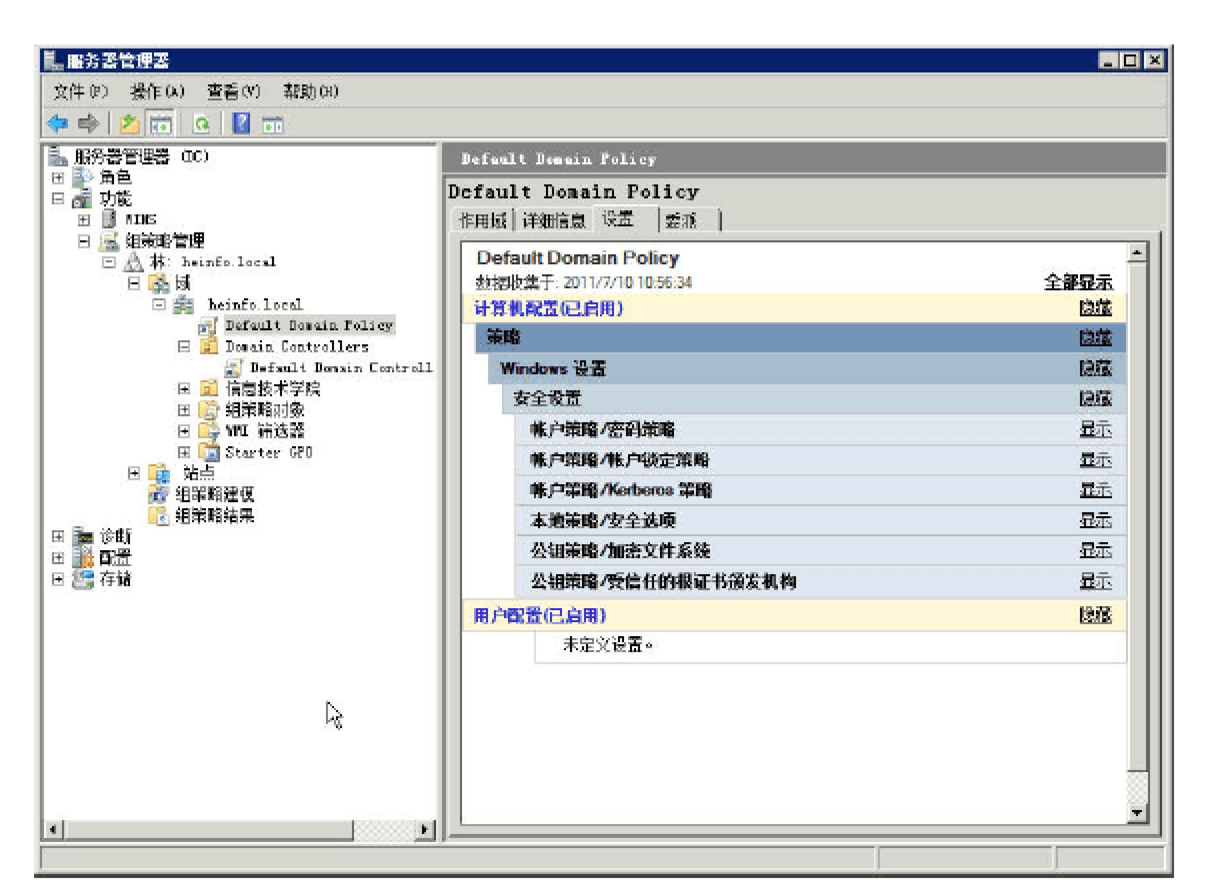


图 8-17　设置

在“委派”选项卡，显示了哪些组和用户拥有此 GPO 的指定权限，如图 8-18 所示。

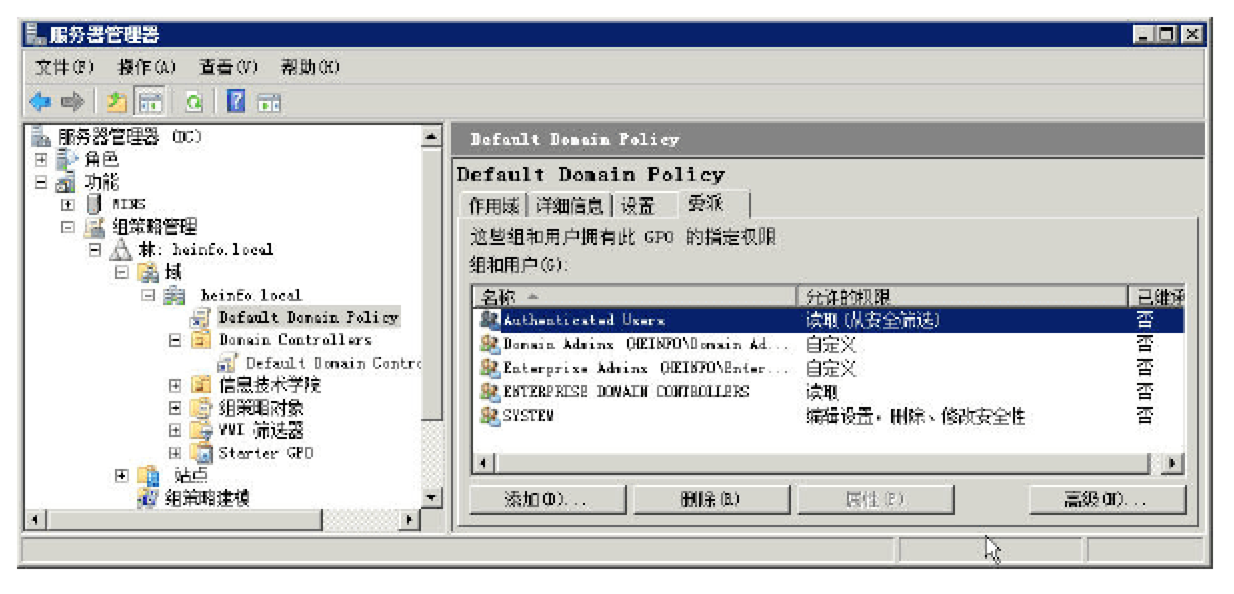


图 8-18　委派

如果要在该组策略中添加例外的用户（即针对该组策略设置不生效的用户），可以在“服务

器管理器”窗口右侧窗格中单击“添加”按钮，添加指定的用户，然后选中该用户，单击“高级”按钮，在弹出的“Default Domain Policy 安全设置”对话框中，选中要排除的用户，为该用户添加“拒绝”权限即可，如图 8-19 所示。

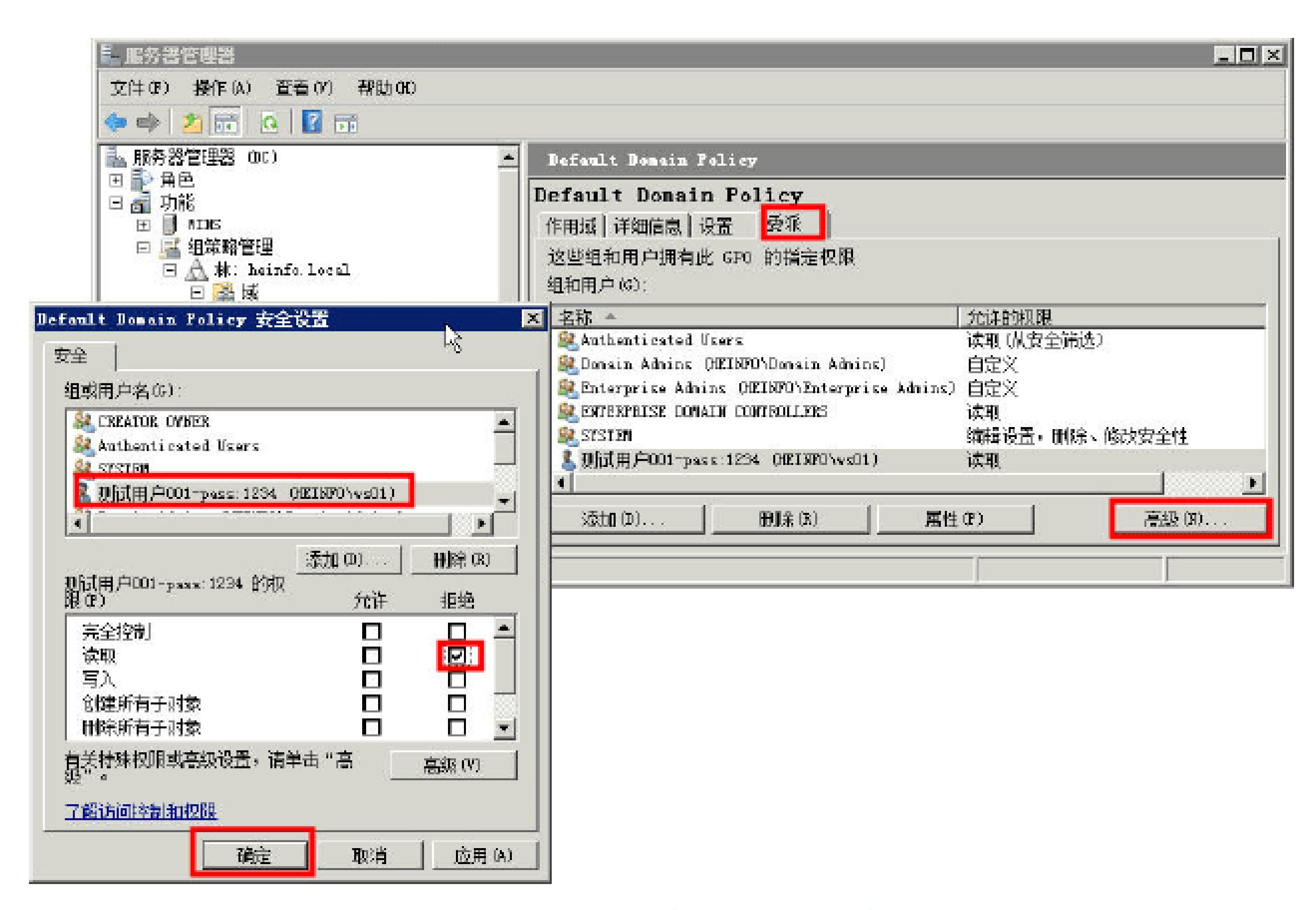


图 8-19 添加例外用户

8.2 创建并编辑组策略

在本节中，我们将介绍组策略的详细使用。如无必要，不要修改默认域策略或默认的域控制器的策略，通常情况下，是在指定的组织单位中创建并链接 GPO。

8.2.1 创建组策略并进行链接

接下来，将在“信息技术学院”组织单位中，创建 GPO 并进行链接，步骤如下。

01 在“服务器管理器”中，定位到“功能→组策略管理→林→域→（域名）”，右击“信息技术学院”，在弹出的快捷菜单中选择“在这个域中创建 GPO 并在此处链接”选项，如图 8-20 所示。

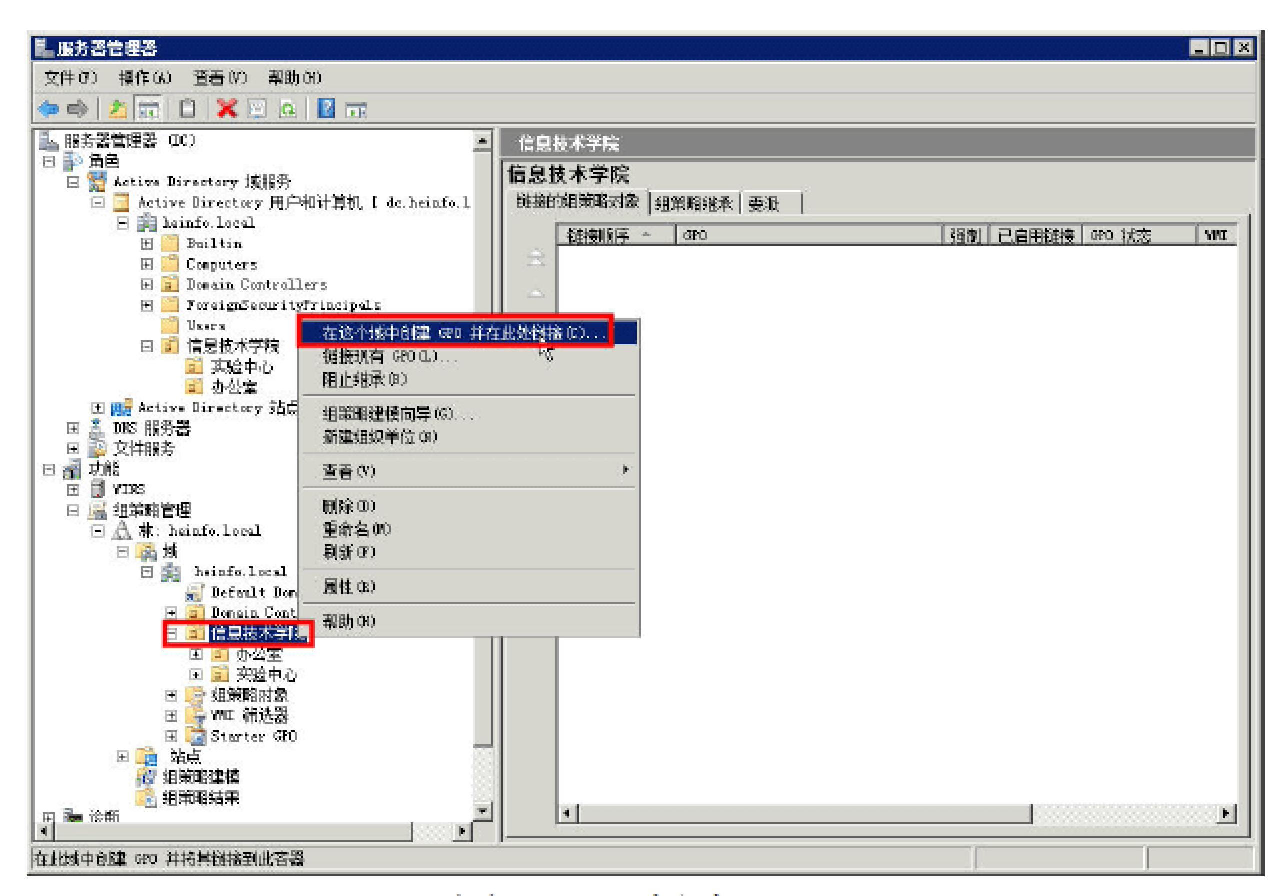


图 8-20 创建 GPO

02 在弹出的“新建 GPO”对话框中，在“名称”文本框中输入新建的 GPO 的名称，在本例为 heinfo（通常情况下，创建的 GPO 名称要与对应的 OU 具有一定的关系，以方便后期的管理），然后单击“确定”按钮，如图 8-21 所示。

03 创建 GPO 后，在右侧选中创建的 GPO，用鼠标右击，在弹出的快捷菜单中，选择对应的命令，如图 8-22 所示。在此选择“编辑”，也可以删除、重命名这个 GPO。

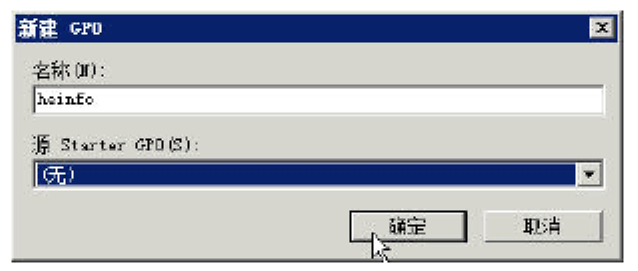


图 8-21　新建 GPO

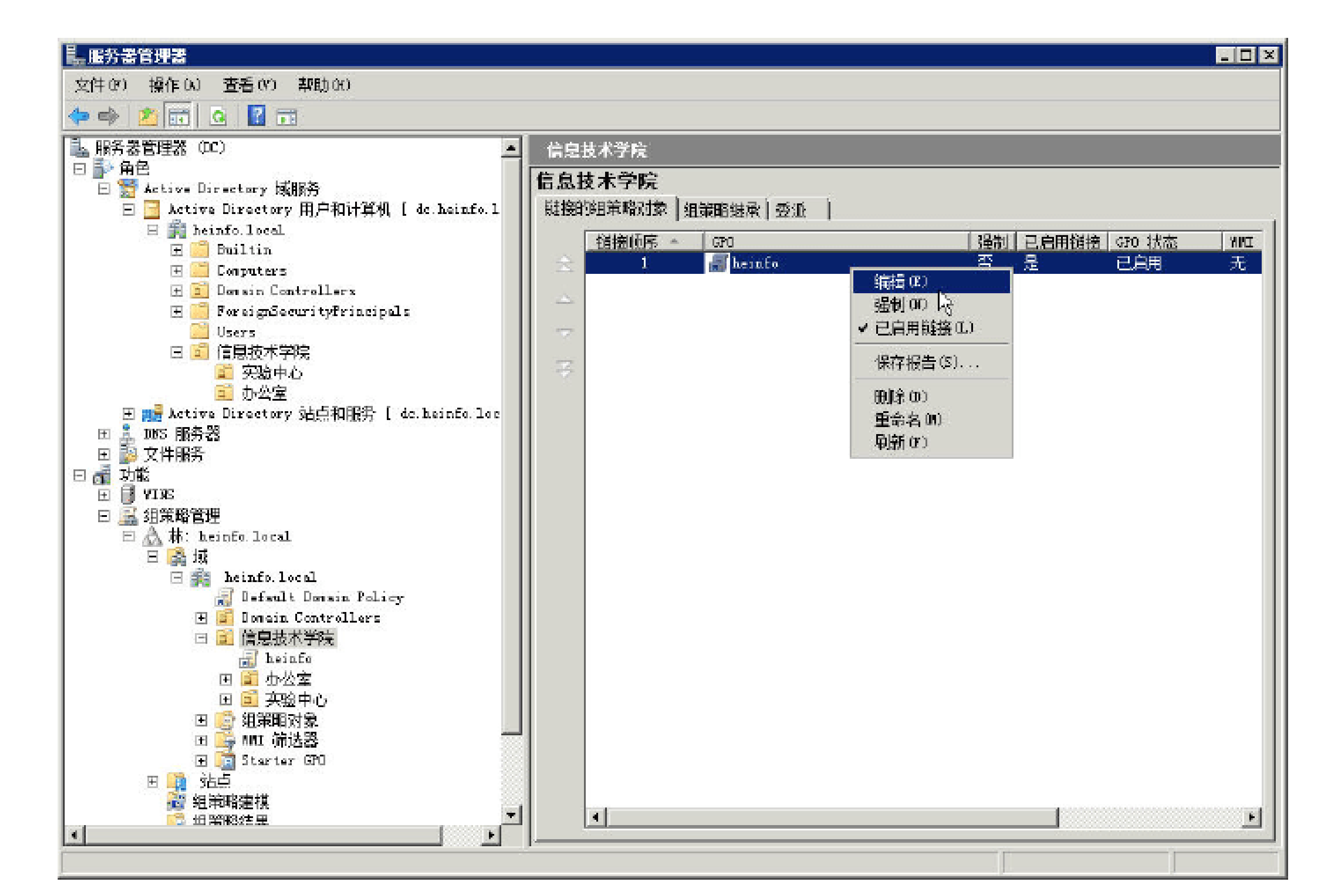


图 8-22　编辑 GPO

04 随后将打开“组策略管理编辑器”窗口，该策略将会应用于“信息技术学院”组织单位中所属的用户、用户组及计算机对象。如图 8-23 所示。

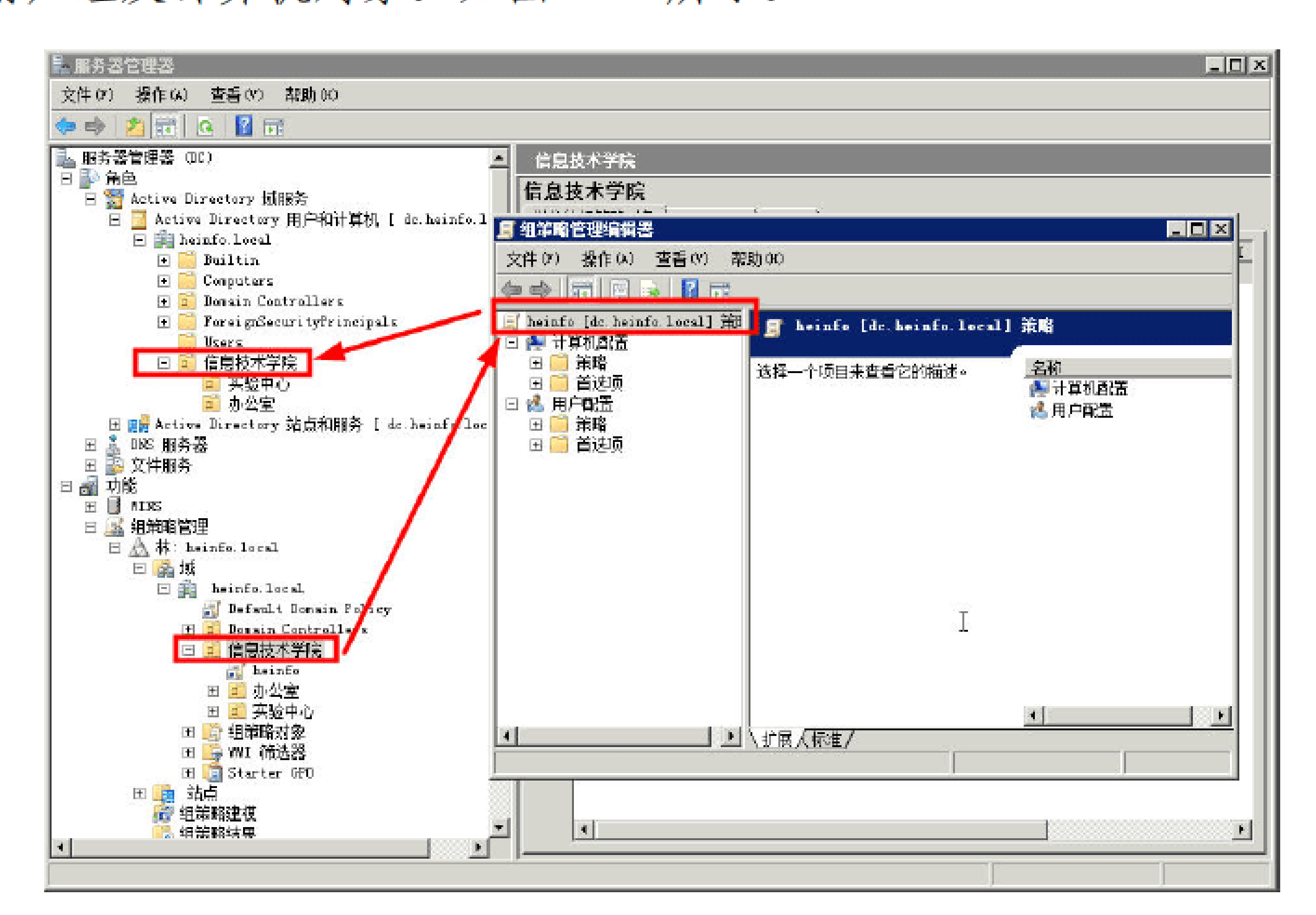


图 8-23　组策略管理应用

8.2.2　计算机配置与用户配置

打开“组策略管理编辑器”后，可以看到，每个组策略包括“计算机配置”与“用户配置”，如图 8-24 所示。

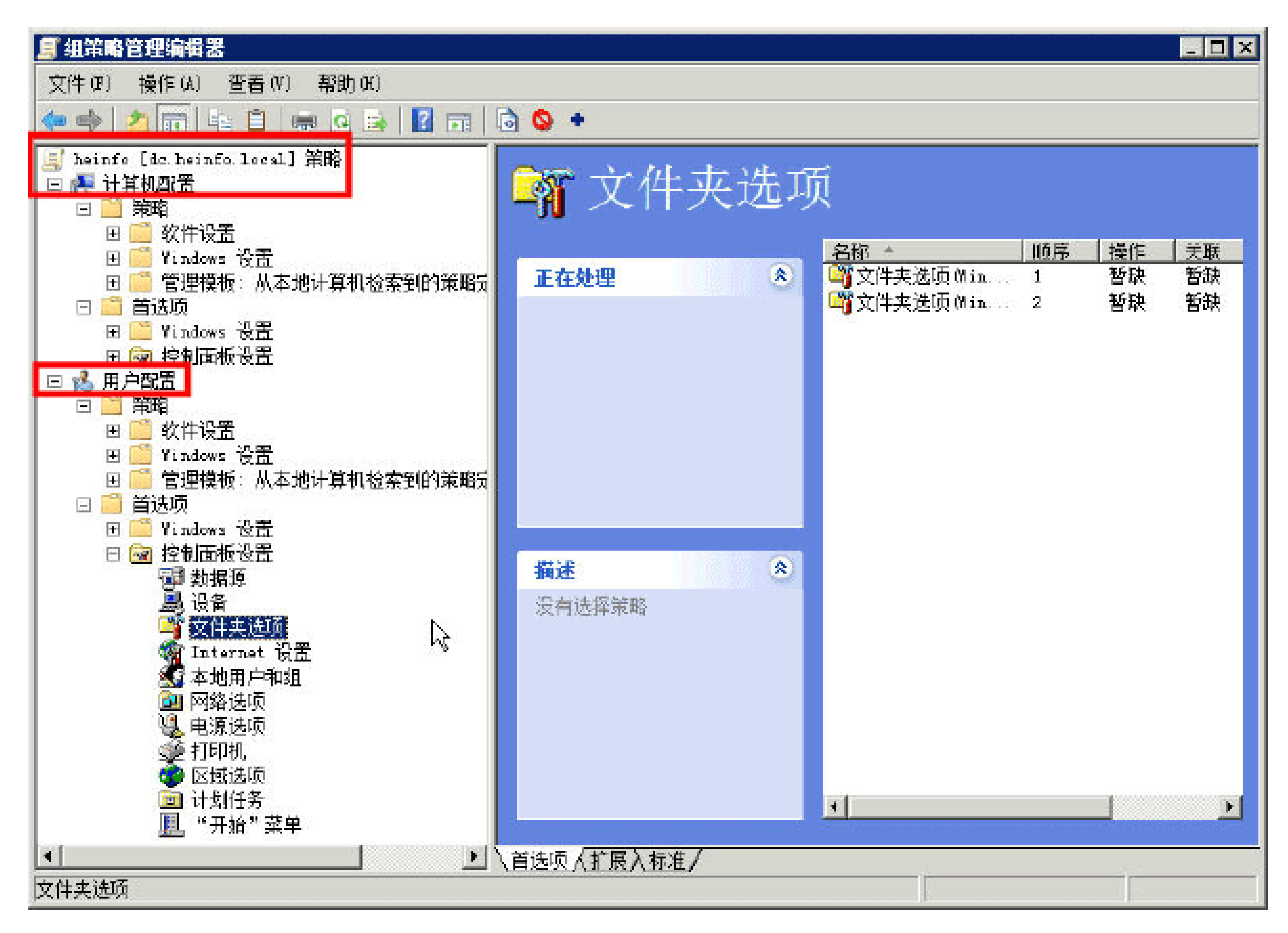


图 8-24 组策略管理编辑器

在组策略中，策略可以应用于“计算机配置”或“用户配置”，且在“计算机配置”中的策略将只能用于“计算机”，而“用户配置”中的策略将只能用于“用户”。

例如：在本例中，是在“信息技术学院”组织单位中，创建的组策略。目前在“信息技术学院”中，只有 heinfo-admin、ws01、ws02 等 3 个用户和 wg01 组（如图 8-25 所示），没有“计算机对象”，如果修改或编辑“计算机配置”中的策略，由于当前组织单位中没有“计算机”，所以该策略将没有意义。如果要使用“计算机配置”策略，可以从“heinfo.local→Computers”中，移动计算机到“信息技术学院”组织单位中。

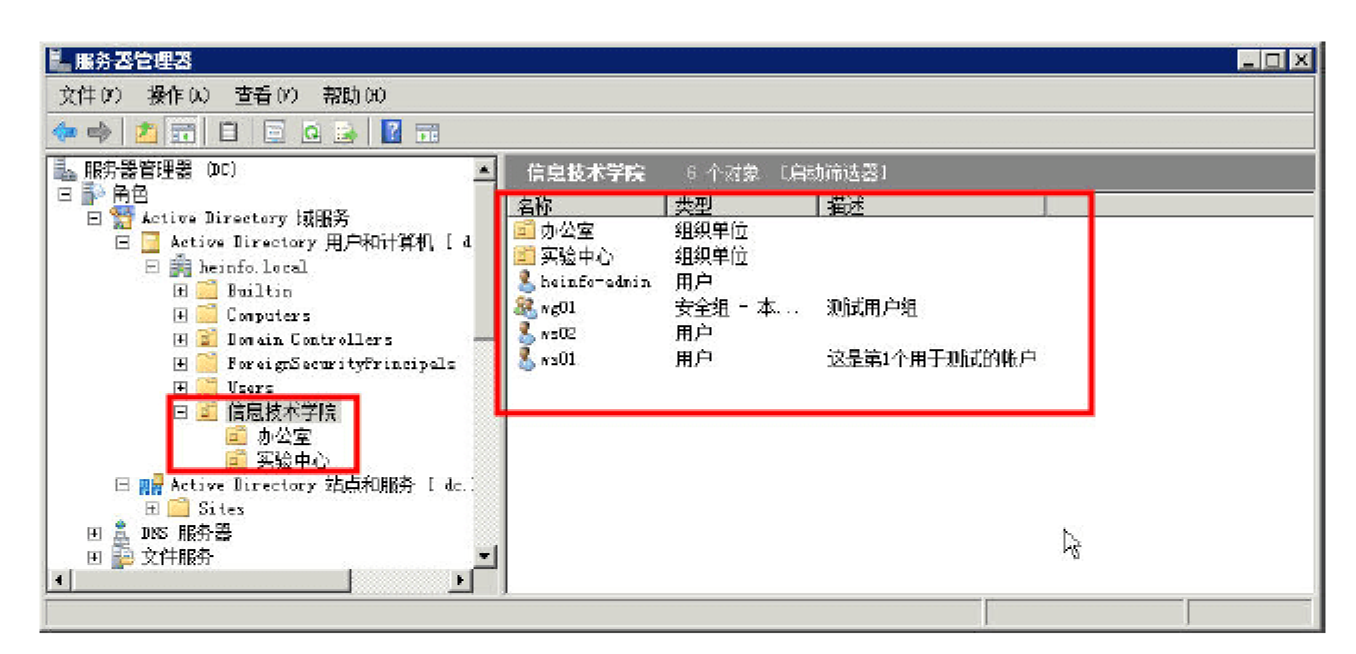


图 8-25 信息技术学院组织单位

由于该组织单位中具有多个用户组，所以在修改了“用户配置”后，使用信息技术学院组织单位中的用户（ws01、ws02、heinfo-admin）或者其中加入到“wg01”组的用户在工作站登录时，将应用该组策略。

说 明

如果“办公室”、“实验中心”子组织单位中存在用户、用户组或计算机对象，则这些对应也会应用该组策略。

无论是“计算机配置”还是“用户配置”，在“策略”中都包括“软件设置”、“Windows 设置”与“管理模板”，在每一个子项中，具体的设置策略可能相同，也可能不同（例如，在“计

算机配置→策略→Windows 设置”中没有“文件夹重定向”的策略，而在“用户配置→策略→Windows 设置”中则有）。如果有相同的策略并且设置互相矛盾时，以“计算机配置”为准。

在有多个组织单位时，如果某组织单位没有创建策略，则会继承上一层的策略，如果上一层组织单位没有策略，会从上上一层继承，直到从“默认域策略”继承。如果某个组织单位既有自己这一层的策略，也有上一层的策略时，如果策略不冲突，则同时生效（即在上一层中设置的策略、本层没有创建类似的策略）；如果策略冲突，则以本层的策略为准。

8.2.3 策略与首选项的区别

在“计算机配置”与“用户配置”中，都包括“策略”与“首选项”，这两者的区别是：

（1）首选项允许用户使用熟悉的组策略管理控制台管理所有附加设置。在大多数首选项中，用户界面模仿相关的最终用户界面来配置设置，从而使配置更加直观。首选项并非强制性的应用，它相当于客户端的“默认”设置，客户端可根据需要更改这些设置。而策略设置是强制性的应用，客户端一旦应用这些设置后，将不能更改。

（2）如果要筛选“策略设置”，必须针对整个 GPO 来筛选；而“首选项”可以针对单一设置项目进行设置。

首选项提供 20 多个组策略扩展，它们扩展组策略对象中的可配置首选项设置的范围。组策略允许用户管理驱动器映射、注册表设置、本地用户和组、服务、文件和文件夹，而不需要学习脚本语言。

在 Windows 7、Windows Server 2008、Windows Server 2008 R2 的客户端计算机，已经支持首选项的客户端设置。如果是 Windows Vista 及其以前的计算机，要应用“首选项”设置，必须从 http://technet.microsoft.com/zh-cn/library/cc731892（WS.10）.aspx 下载该客户端扩展功能。

8.3 常用策略及应用

在 Windows Server 2003、Windows Server 2008、Windows Server 2008 R2 中，组策略的项目非常多，如果要详细的介绍每一条策略，将会占用大量的篇幅（可能需要写几百页的一本书来讲述），而在 Windows Server 中，操作系统本身的“帮助”功能也非常的强大，许多时候，用户可以通过在线的帮助，来查看具体每条策略的意义以及设置项。所以，本节将介绍相对重要的策略，其他没有介绍的策略，请读者通过帮助进行学习并进行测试。

在组策略应用中，无论是“计算机配置”还是“用户配置”，都有“软件设置”这一条策略。这条策略我们将在下一节单独并详细的介绍。首先，我们介绍其他常用的及比较重要的策略。

8.3.1 账户策略

在“组策略管理编辑器”窗口中，定位到“计算机配置→策略→Windows 设置→安全设置”中的“账户策略”，包括“密码策略”、“账户锁定策略”与“Kerberos 策略”，而在“密码策略”中包括“密码必须符合复杂性要求”、“密码长度最小值”、“密码最短使用期限”、“密码最长

使用期限”、“强制密码历史”、“用可还原的加密来储存密码”等策略，如图 8-26 所示。

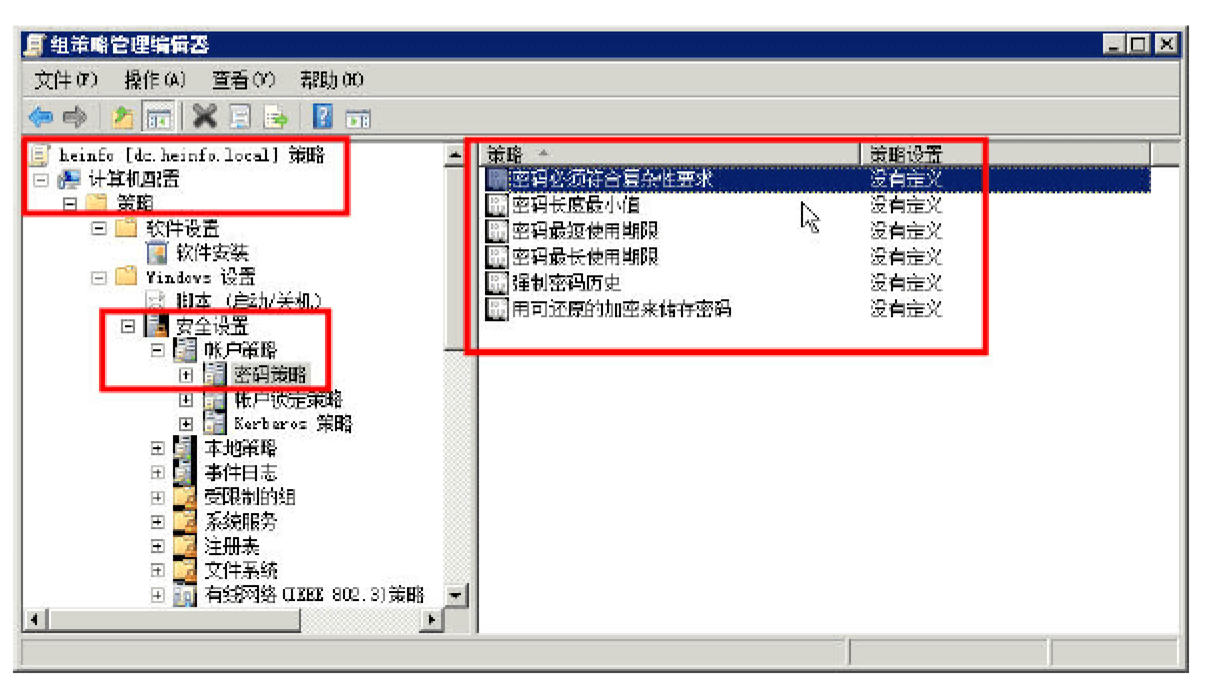


图 8-26　密码策略

在默认情况下，成员计算机沿用各自域控制器的配置。如果要修改这些策略，只须直接用鼠标双击想要修改的策略，例如双击“密码必须复合复杂性要求”，在弹出的“密码必须符合复杂性要求　属性”对话框中，选中“定义这个策略设置”复选框，并根据需要，选择“已启用”（如图 8-27 所示）或“已禁用”选项。如果选择“已启用”，则要求该组织单位中的用户的密码，必须符合“复杂密码要求”；如果选择“已禁用”，则要求该组织单位中的用户密码，不必符合“复杂密码要求”。如果要查看这条策略对应的意义，可以单击“说明”选择卡，在该选项卡中，有该条策略的意义说明，如图 8-28 所示。

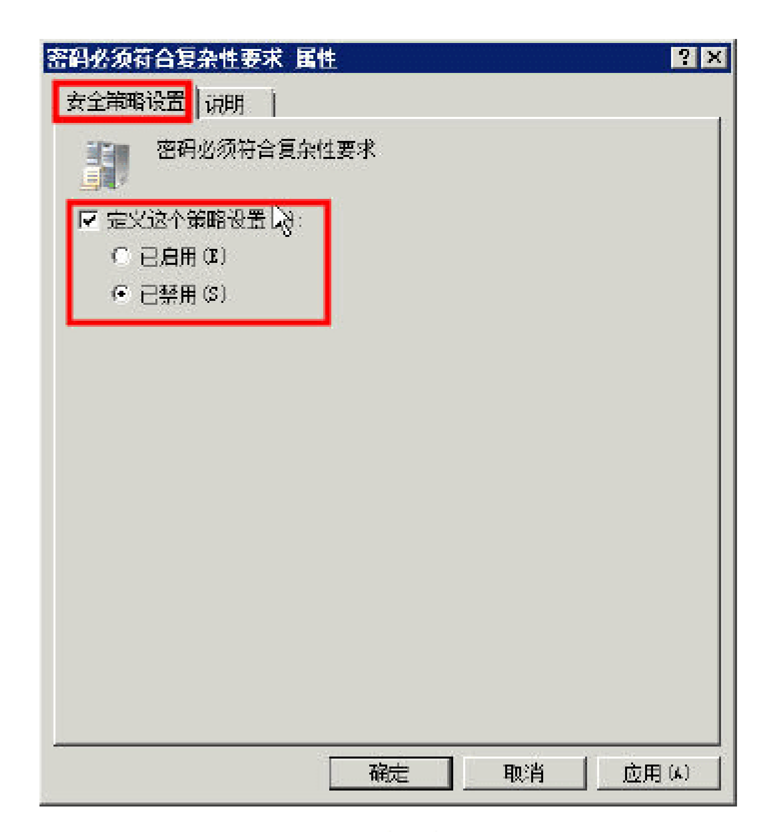


图 8-27　安全策略设置

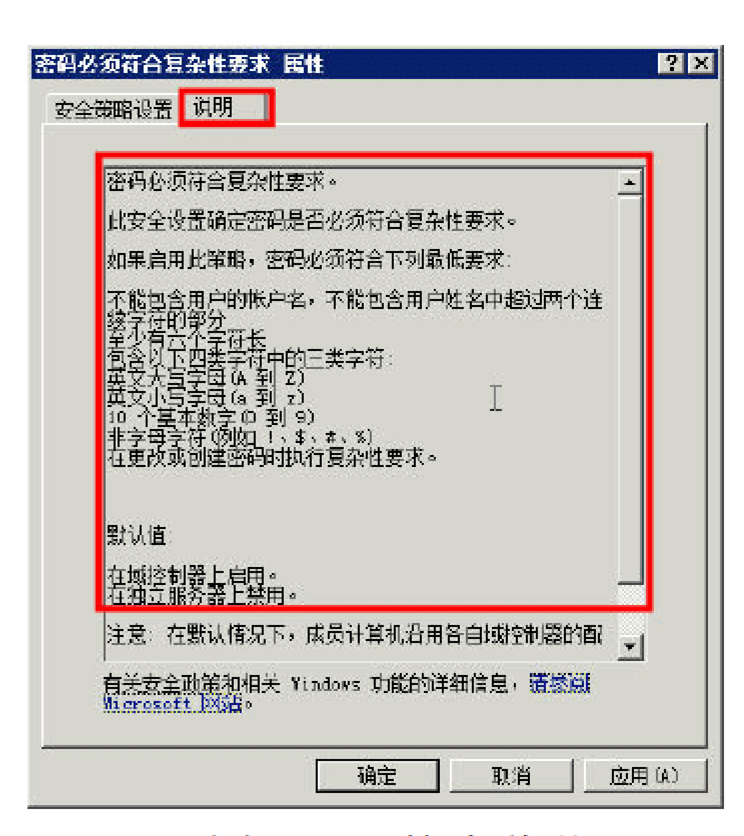


图 8-28　策略说明

在修改策略之后单击“确定”按钮确认，或者单击“取消”按钮，放弃策略的更改。在更改策略之后，返回到“组策略编辑管理器”窗口，继续修改或查看其他的策略。

8.3.2　本地策略

在“组策略管理编辑器”窗口中，定位到“计算机配置→策略→Windows 设置→安全设置”中的“本地策略”，包括“审核策略”、“用户权限分配”与“安全选项”3 个子策略组，其中“用户权限分配”策略组中，可以修改实现某些功能的用户或组，例如“备份文件和目录”策略中，可以添加具有“备份文件和目录”权限的用户或组。

在“用户权限分配”策略中，包括“备份文件和目录”、“充当操作系统的一部分”、“创

建符号链接”等多个策略，如图 8-29、图 8-30 所示。

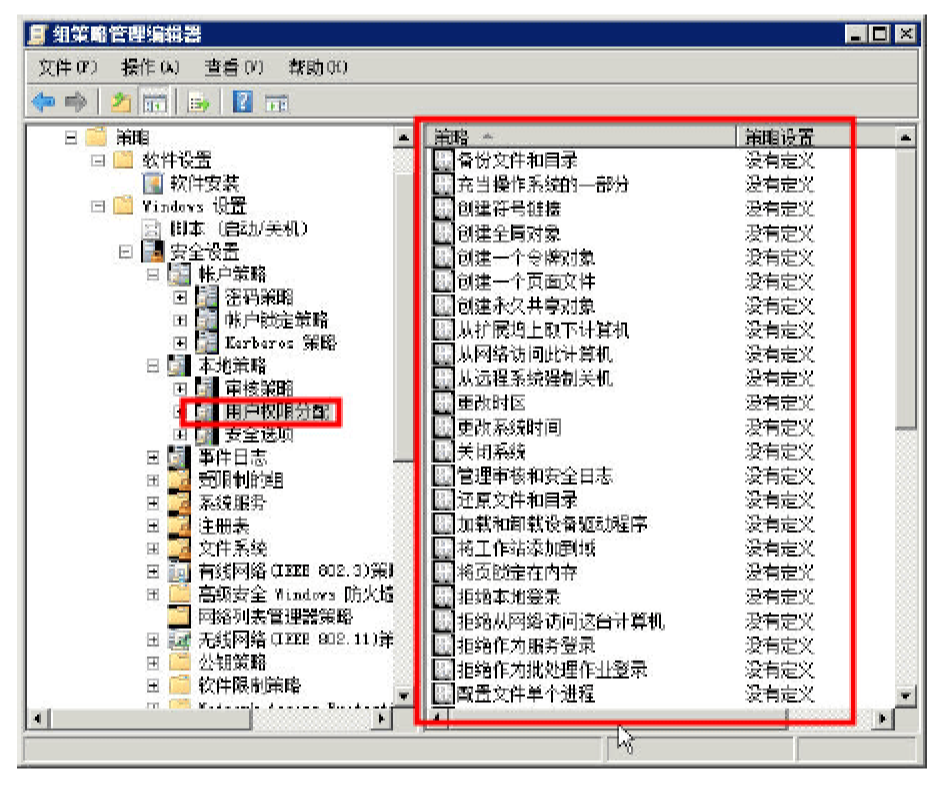


图 8-29　用户权限分配策略 1

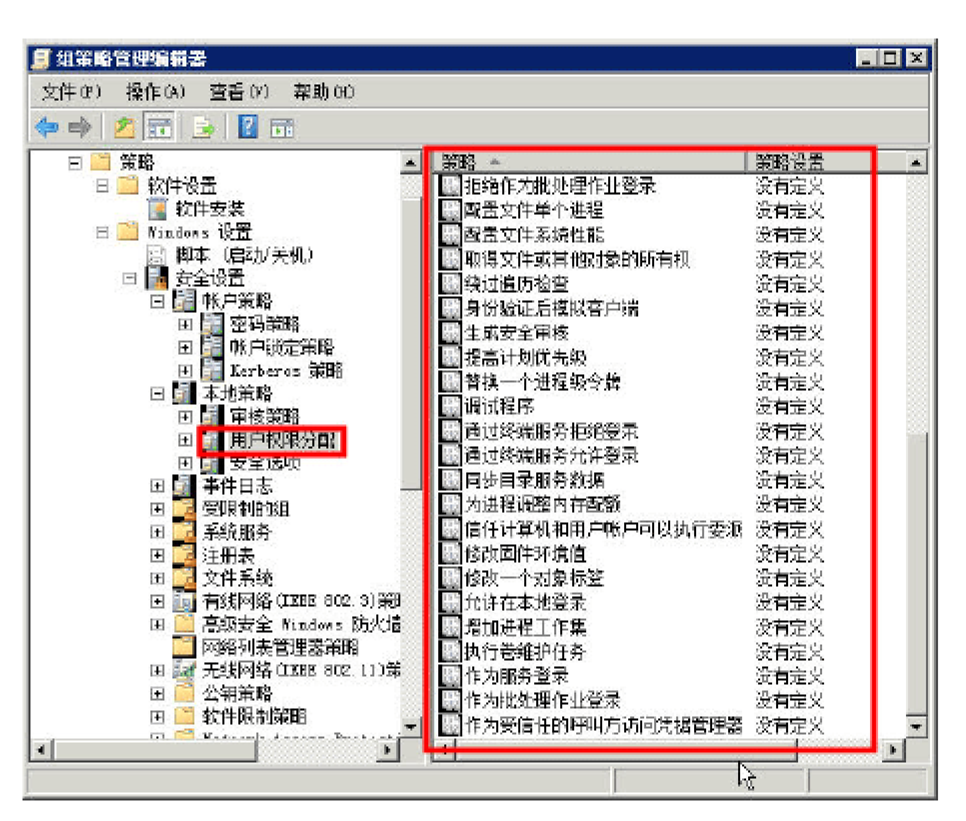


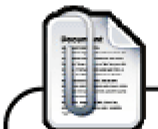
图 8-30　用户权限分配策略 2

在这些策略中，比较重要的策略有：

（1）将工作站添加到域。在修改这条策略时，如图 8-31 所示，默认情况下，任何已经通过身份验证的用户都具有此权限并可以在该域中最多创建 10 个计算机账户。



图 8-31　将计算机添加到域



说　明

在“8.1.2 委派用户权限”一节中，介绍了委派用户权限、指定用户将计算机加入到域的权限。该设置与 8.1.2 一节中的区别在于，在 Active Directory 用户和计算机容器上具有权限的用户并不受限于仅创建 10 个计算机账户。

（2）允许在本地登录。此登录权限确定哪些用户能以交互方式登录到此计算机。通过在计算机的键盘上按 Ctrl+Alt+Del 序列启动的登录要求用户具有此登录权限。在默认情况下，只有 Administrators、Backup Operators 等组的用户才有“在本地登录”的权限。

在“本地策略→安全选项”中，设置与服务器或域控制器安全相关的登录，例如“交互式登录：不显示最后的用户名”、“交互式登录：试图登录的用户的消息标题”、“交互式登录：提示用户在过期之间更改密码”、“交互式登录：无须按 Ctrl+Alt+Del”等，如图 8-32 所示。

图 8-32　安全选项

在“安全选项”策略组中，常用的策略有：

（1）交互式登录：无须按 Ctrl+Alt+Del。该安全设置决定用户是否需要按 Ctrl+Alt+Del 才能登录，如图 8-33 所示。如果计算机中启用了此策略，则用户无须按 Ctrl+Alt+Del 便可登录，但启用此策略会使用户易于受到企图截获用户密码的攻击。用户登录之前需按 Ctrl+Alt+Del 可确保用户输入其密码时通过信任的路径进行通信。如果禁用了此策略，则任何用户登录 Windows 之前都需要按 Ctrl+Alt+Del（除非他们使用智能卡进行 Windows 登录）。

（2）使用空白密码的本地账户只允许进行控制台登录，如图 8-34 所示。如果启用此项设置，使用空白密码（即无密码的账户）只能用于从计算机的键盘上登录。如果禁用此项设置，使用空白密码的账户可能通过网络（例如使用共享文件夹）访问此服务器，也可以用于远程登录（例如使用远程桌面）。

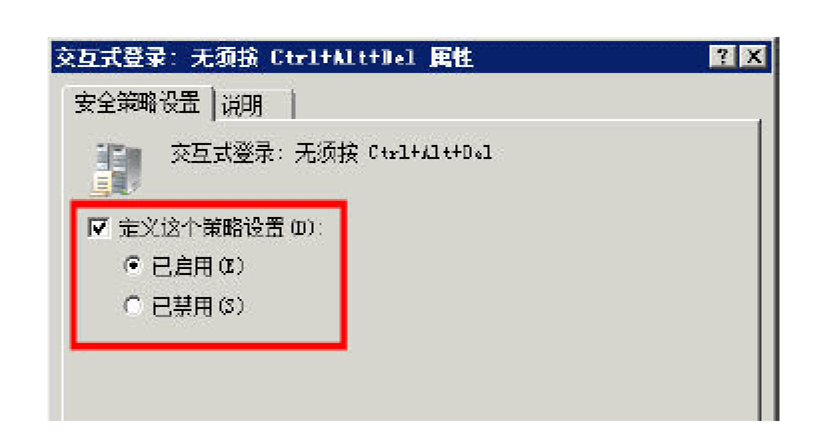


图 8-33　无须按 Ctrl+Alt+Del

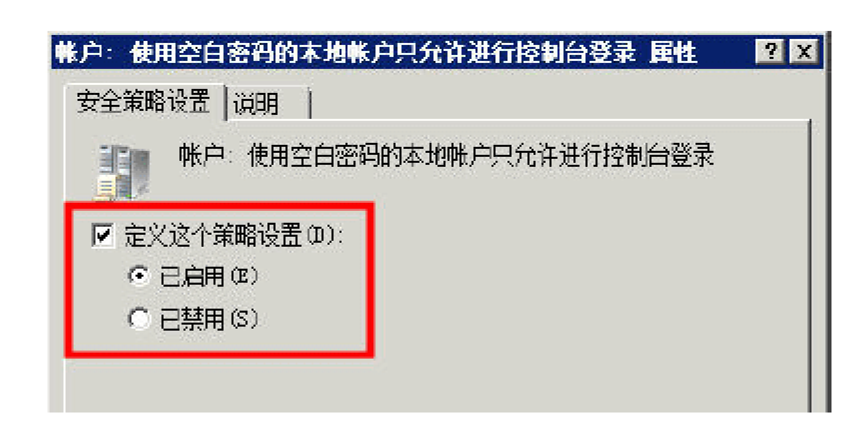


图 8-34　使用空白密码的本地账户只允许进行控制台登录

说 明

大家可能听说过一句话，在 Windows XP 中，没有密码比有密码更安全。因为在 Windows XP、Windows Server 2003 开始，“使用空白密码的本地账户只允许进行控制台登录”的策略是默认启用的，如果这些系统的管理员账户没有设置密码，由于只允许控制台登录，而禁止网络访问，所以即使有黑客攻击，也比较安全。如果设置了相对简单的密码并被他人知道的话，计算机上的数据就会被他人通过“共享文件夹”或其他方式窃取。

8.3.3　高级安全 Windows 防火墙

在“组策略管理编辑器”窗口中，定位到“安全设置→高级安全 Windows 防火墙”策略组中，可以配置“高级安全 Windows 防火墙”的策略，包括“入站规则”、“出站规则”以及“连接安全规则”，本小节以创建“文件和打印机共享”的入站规则为例，介绍高级安全 Windows 防火墙策略

组的配置。

01 在左侧任务窗格定位到“安全设置→高级安全 Windows 防火墙→高级安全 Windows 防火墙→入站规则”，在右侧窗格中空白位置右击，在弹出的快捷菜单中选择“新规则”选项，如图 8-35 所示。

02 在“规则类型”对话框中，选中“预定义”单选按钮，在下拉列表中，选择“文件和打印机共享”选项，如图 8-36 所示。

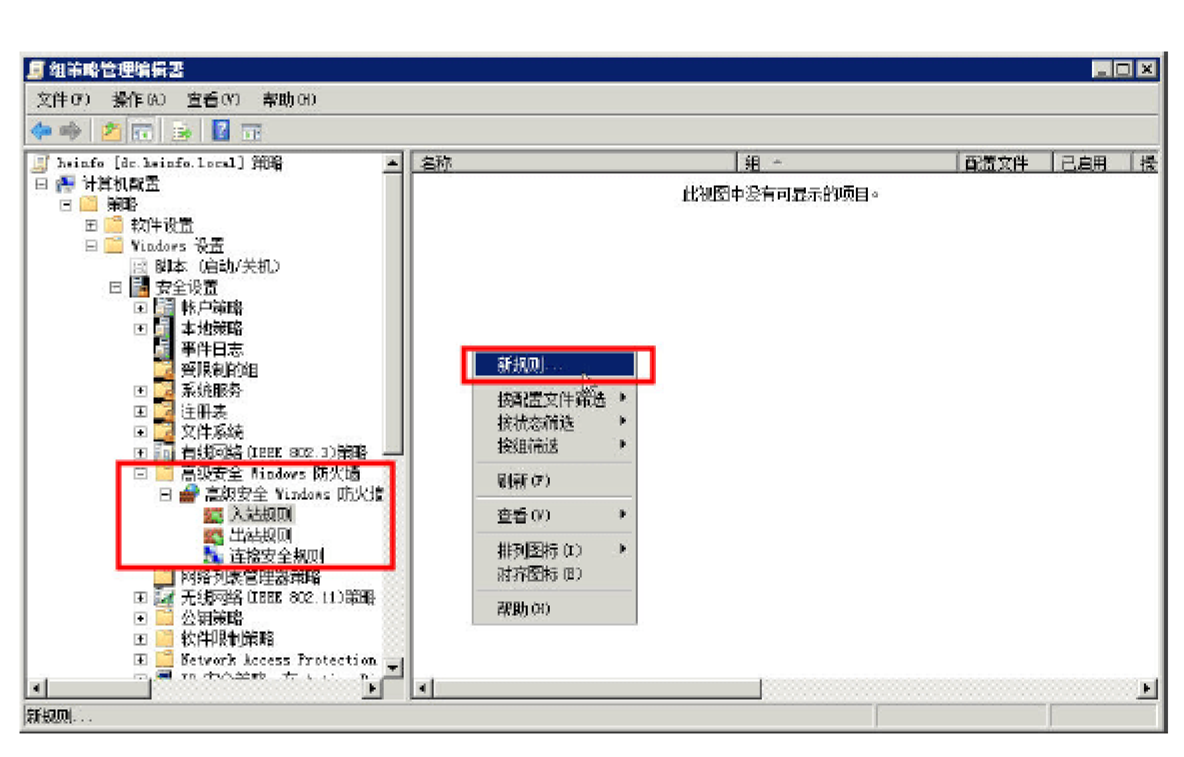


图 8-35 新规则

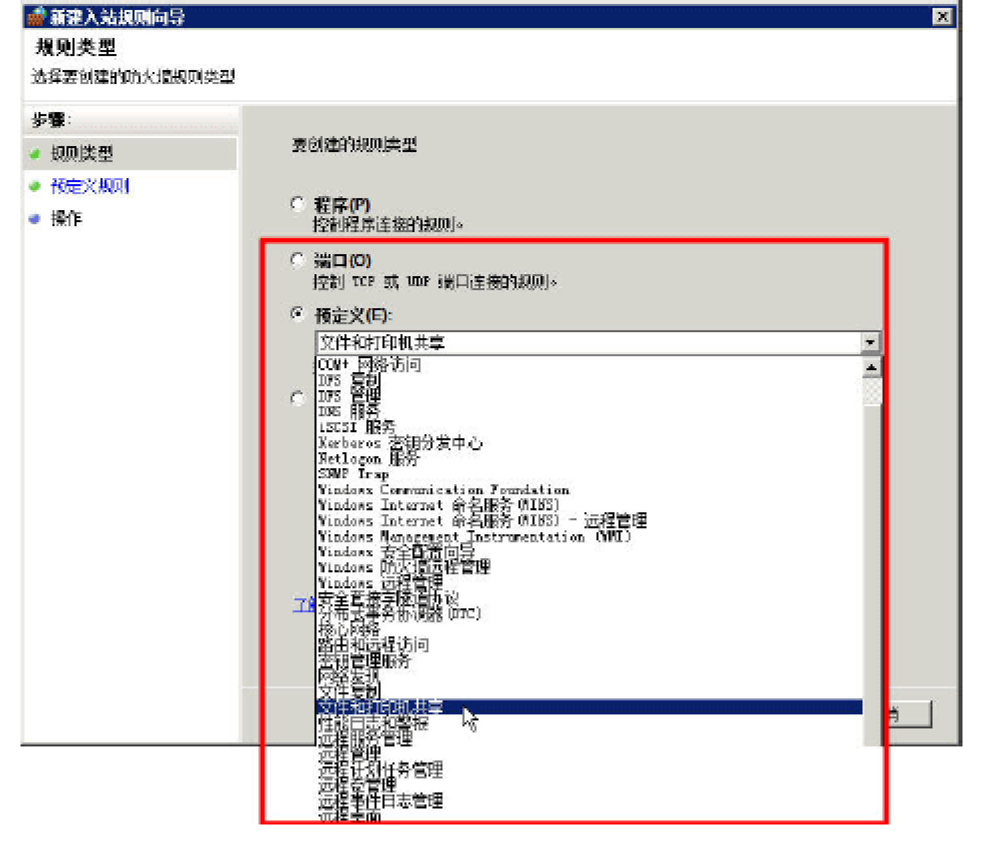
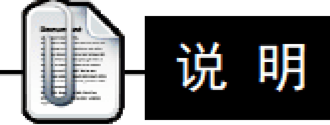


图 8-36 文件和打印机共享



说 明

在“预定义”列表中，列出了大部分常用的规则，一般情况下从列表中即可以找出所需要的规则。

03 在“预定义规则”对话框中，显示了要创建的规则，通常选择默认值即可，如图 8-37 所示。

04 在“操作”对话框中，选择“允许连接”，如图 8-38 所示。



图 8-37 预定义规则



图 8-38 允许连接

05 创建完规则后，返回组策略管理编辑器。

如果要创建自定义的规则，例如，创建 TCP80 与 TCP3389 的规则，可以按照如下的方式创建。

01 在左侧任务窗格定位到“安全设置→高级安全 Windows 防火墙→高级安全 Windows 防火墙→入站规则”中，在右侧窗格中空白位置右击，在弹出的快捷菜单中选择“新规则”选项，在“规则类型”对话框中，选中“端口”单选按钮。

02 在“协议和端口”对话框中，选择该规则用于 TCP 还是 UDP，在本例选择 TCP，然后选择“特定本地端口”，输入要使用的端口，如果是多个端口，用逗号（，）分开，如图 8-39 所示。

03 在“操作”对话框中，选择“允许连接”。在“配置文件”对话框中，选择默认的设置，如图 8-40 所示。

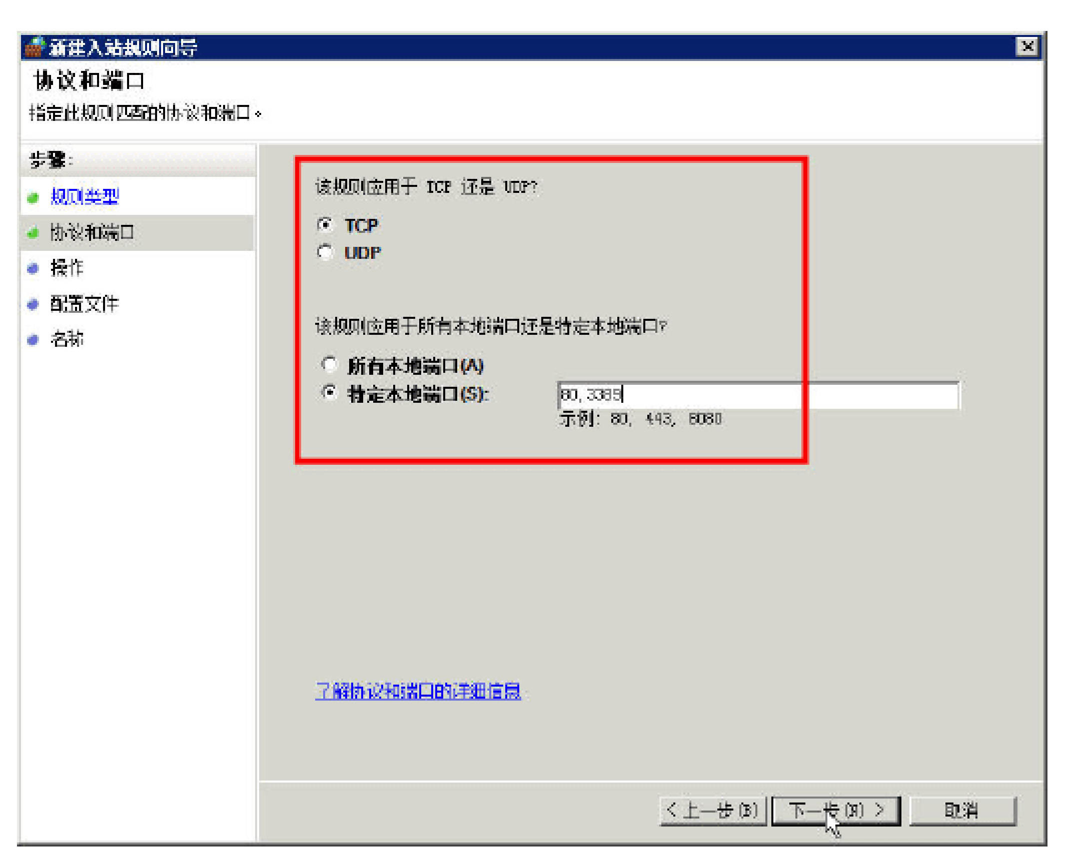


图 8-39　协议和端口



图 8-40　配置文件

04 在“名称”对话框中，为新建规则设置名称，例如 Web-RDP，如图 8-41 所示。

05 创建后的规则如图 8-42 所示。

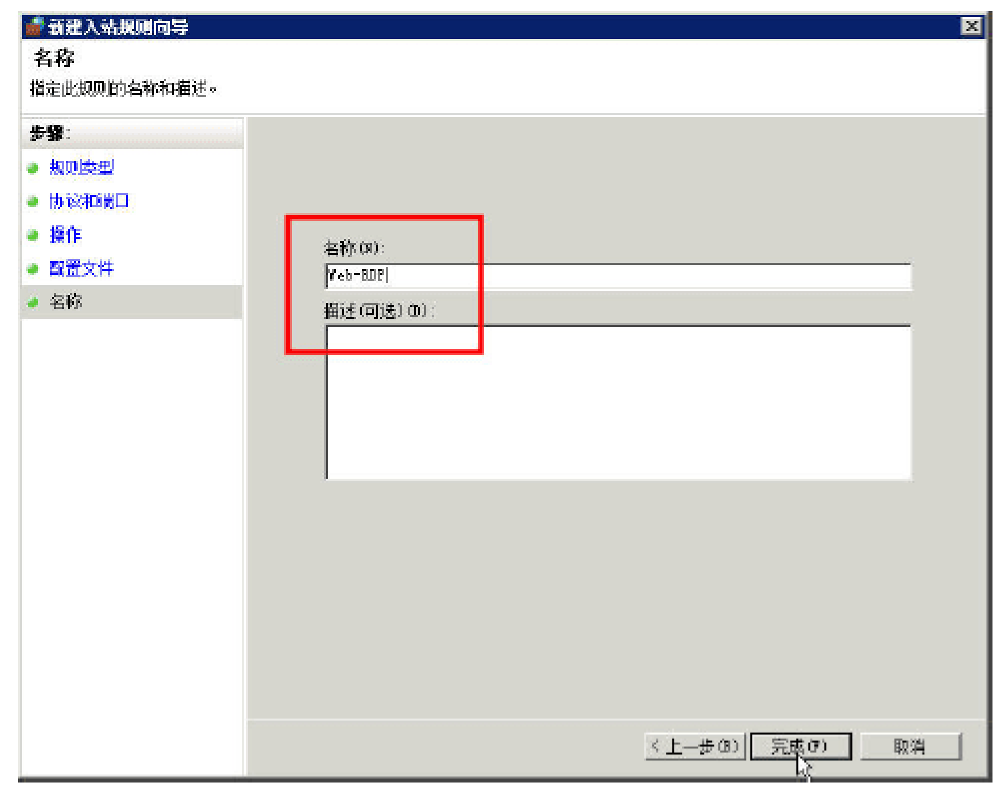




图 8-41　设置规则名称

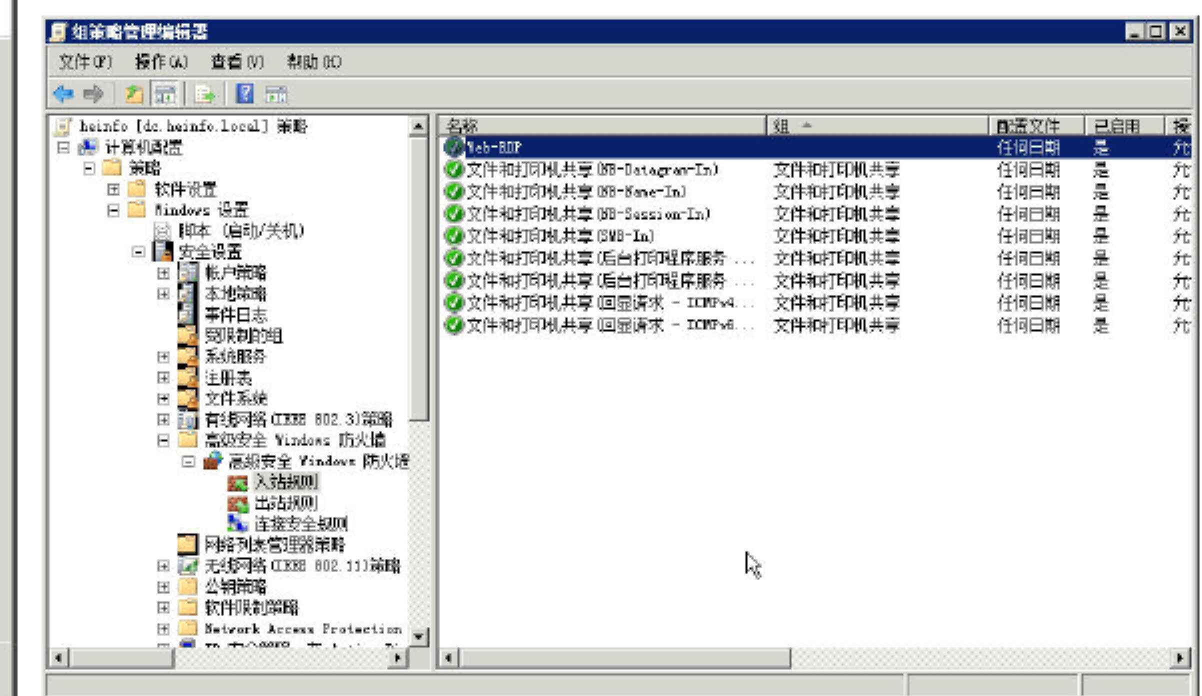


图 8-42　创建规则完成

如果要删除创建的规则，可以用鼠标选中（只能一个一个删除，不能选中多个），按 DEL 键，或者用鼠标单击右键，在弹出的对话框中选择“删除”选项。

8.3.4　计算机配置中的 Internet Explorer 设置

在“组策略管理编辑器”窗口中，定位到“计算机配置→策略→管理模板→Windows 组件”中的“Internet Explorer”策略组，可以定制 Internet Explorer 的设置。

01 在“Internet 控制面板”中，“安全页”与“高级页”分别对应设置 Internet Explorer 的“安全”与“高级”选项卡，在“安全页”中包括的“Internet 区域”、“Intranet 区域”、“受限制的站点区域”、“受信任的站点区域”中每一项设置（如图 8-43 所示），对应 Internet Explorer 浏览器中“安全”选项卡中的配置，如图 8-44 所示。

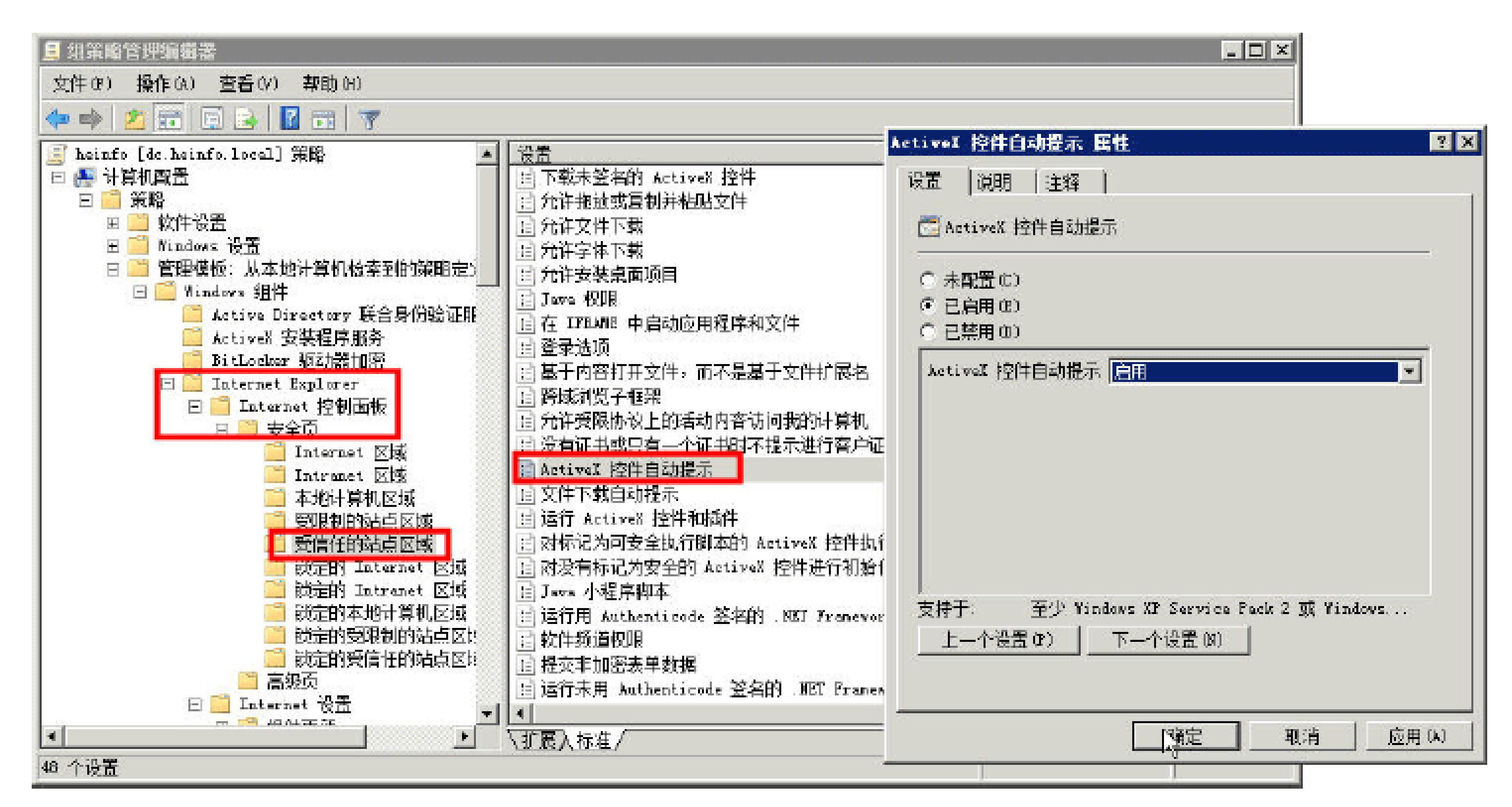


图 8-43　安全页

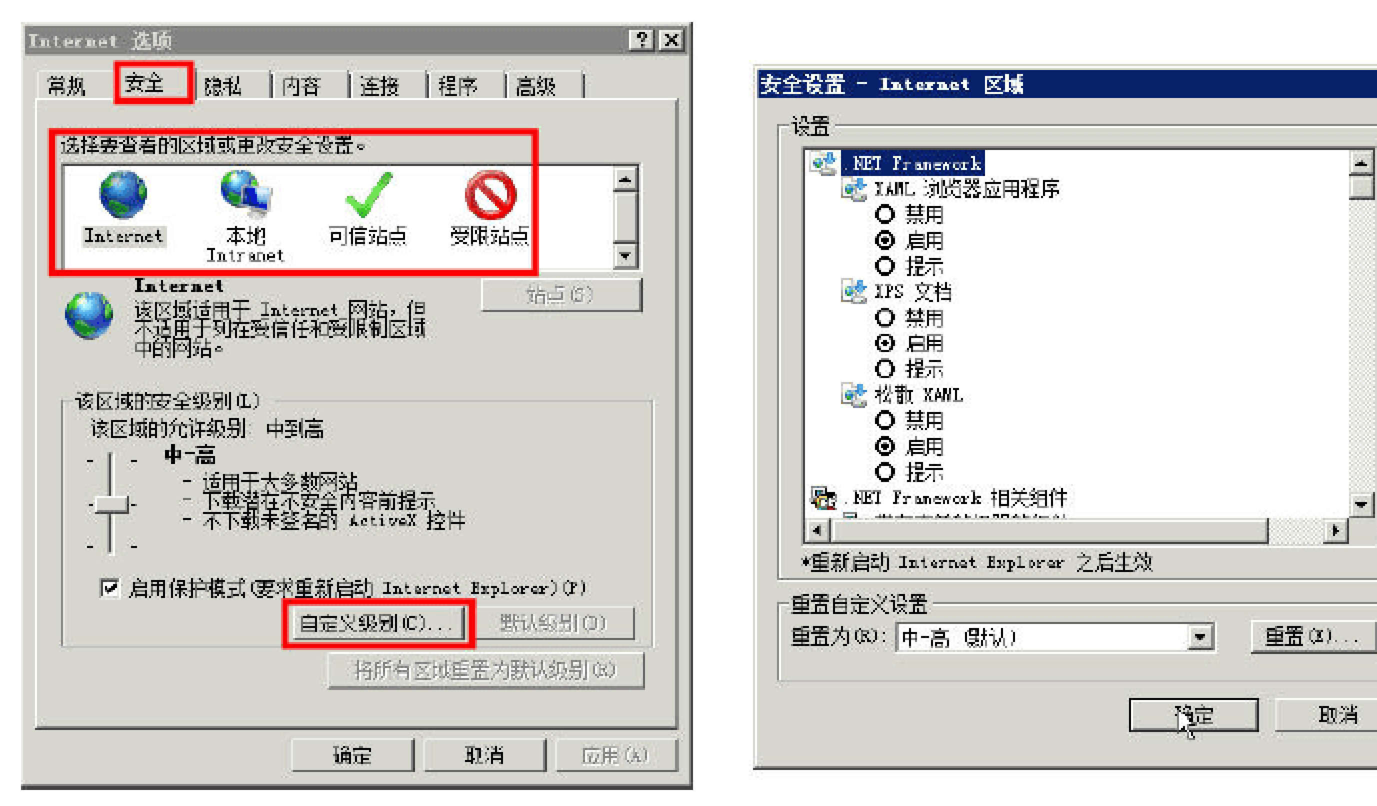
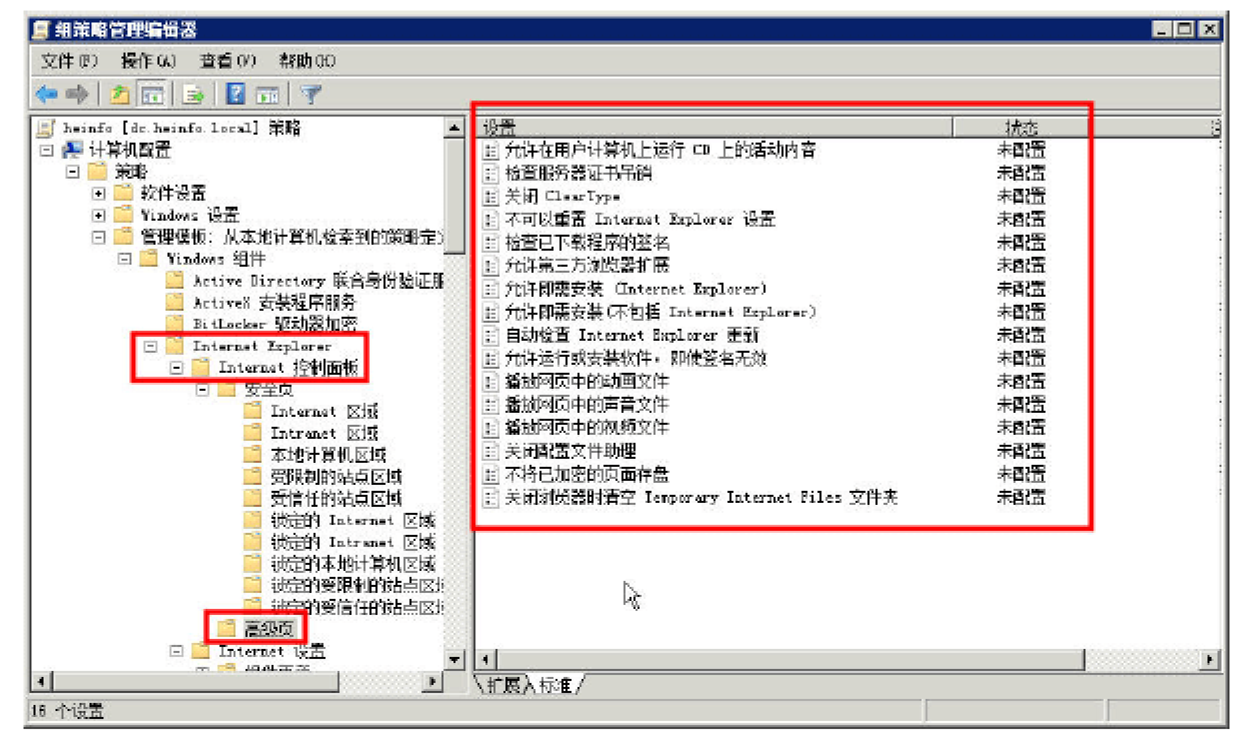


图 8-44　IE 浏览器安全选项卡

02 在“Internet 控制面板→高级页”中（如图 8-45 所示），对应 Internet Explorer 浏览器的“高级”选项卡，如图 8-46 所示。



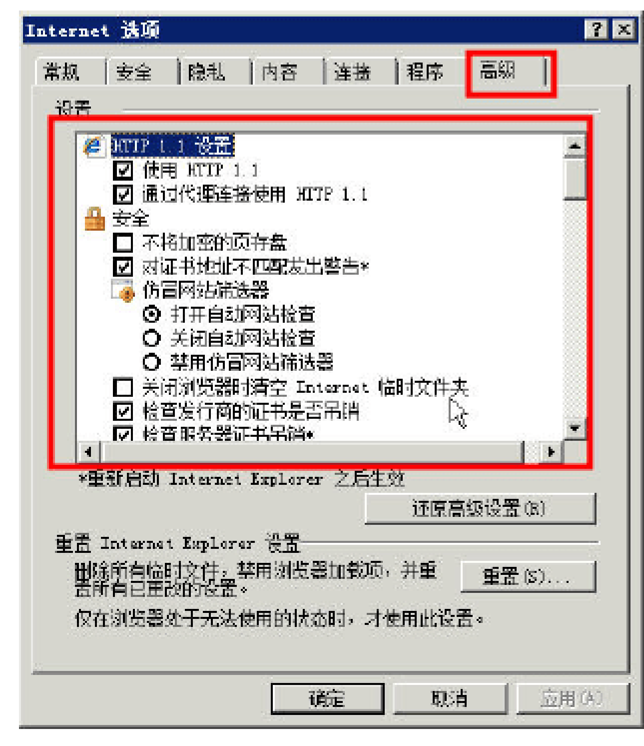


图 8-45　高级页　　图 8-46　高级选项卡

用户可以根据需要，对“安全页”与“高级页”进行设置，从而设置加入到该组织单位中的计算机的 Internet Explorer 的“安全”与“高级”选项卡。

8.3.5 Windows Update 设置

如果网络中有 WSUS 的升级服务器，用户可以在“计算机配置→策略→管理模板→Windows 组件”的“Windows Update”策略组中，设置该组织单位中的“计算机对象”统一使用 WSUS 服务器进行升级，这包括了计算机使用 WSUS 进行升级的各项内容，如图 8-47 所示。

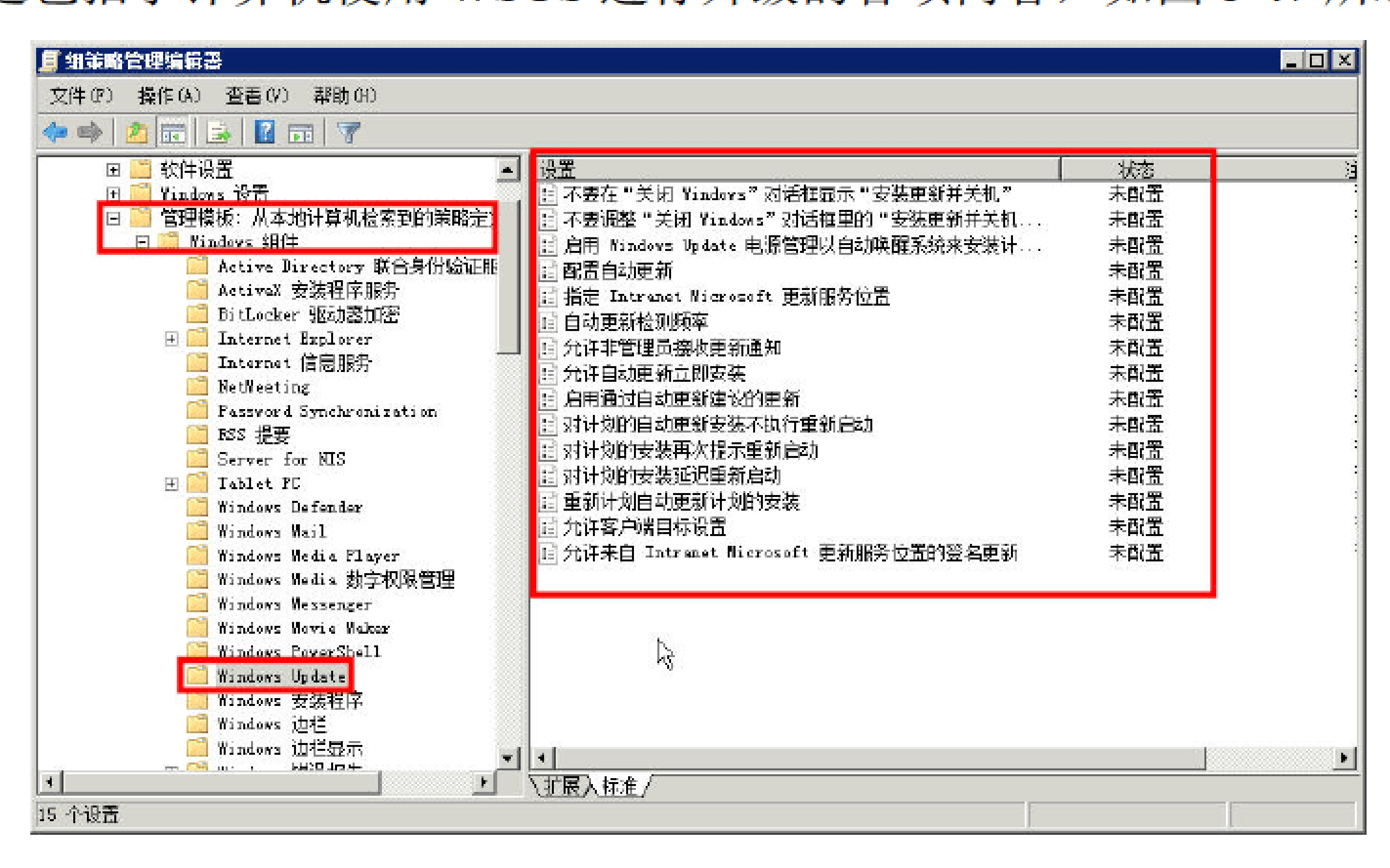


图 8-47 Windows Update 设置

01 在“配置自动更新 属性”对话框的“设置”选项卡中，指定此计算机是否将通过 WSUS 服务器来接收安全更新和其他重要下载，如图 8-48 所示。如果要使用 WSUS，必须选中“已启用”单选按钮，并且在“配置自动更新”列表中，根据你的设置进行选择。

02 在“启动自动更新”后，还要在“指定 Intranet Microsoft 更新服务器位置 属性”对话框中，指定 WSUS 服务器的 IP 地址及服务端口，如图 8-49 所示。在实际使用中，可以使用 WSUS 服务器的计算机名称或 IP 地址替换图中的 wsusip。

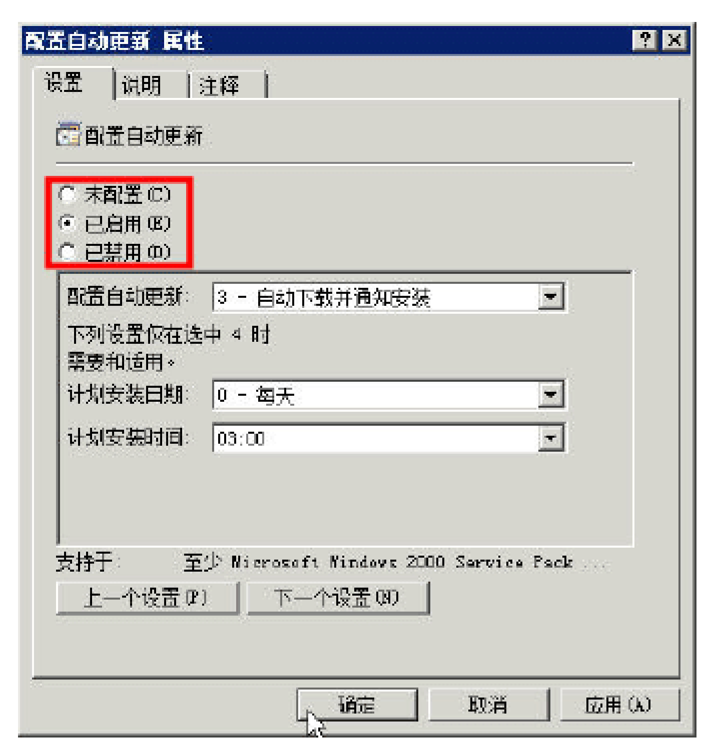


图 8-48 配置自动更新



图 8-49 指定 WSUS 服务器的 IP 地址及服务端口

03 对于 Windows Update 的其他设置，可以通过查看策略帮助进行学习。

8.3.6　终端服务策略

在“组策略管理编辑器”窗口中，定位到“计算机配置→策略→管理模板→Windows 组件”中的“终端服务”策略组，它可以为该组织单位中的所有安装了“终端服务器”的计算机，配置终端服务的策略，如图 8-50 所示。

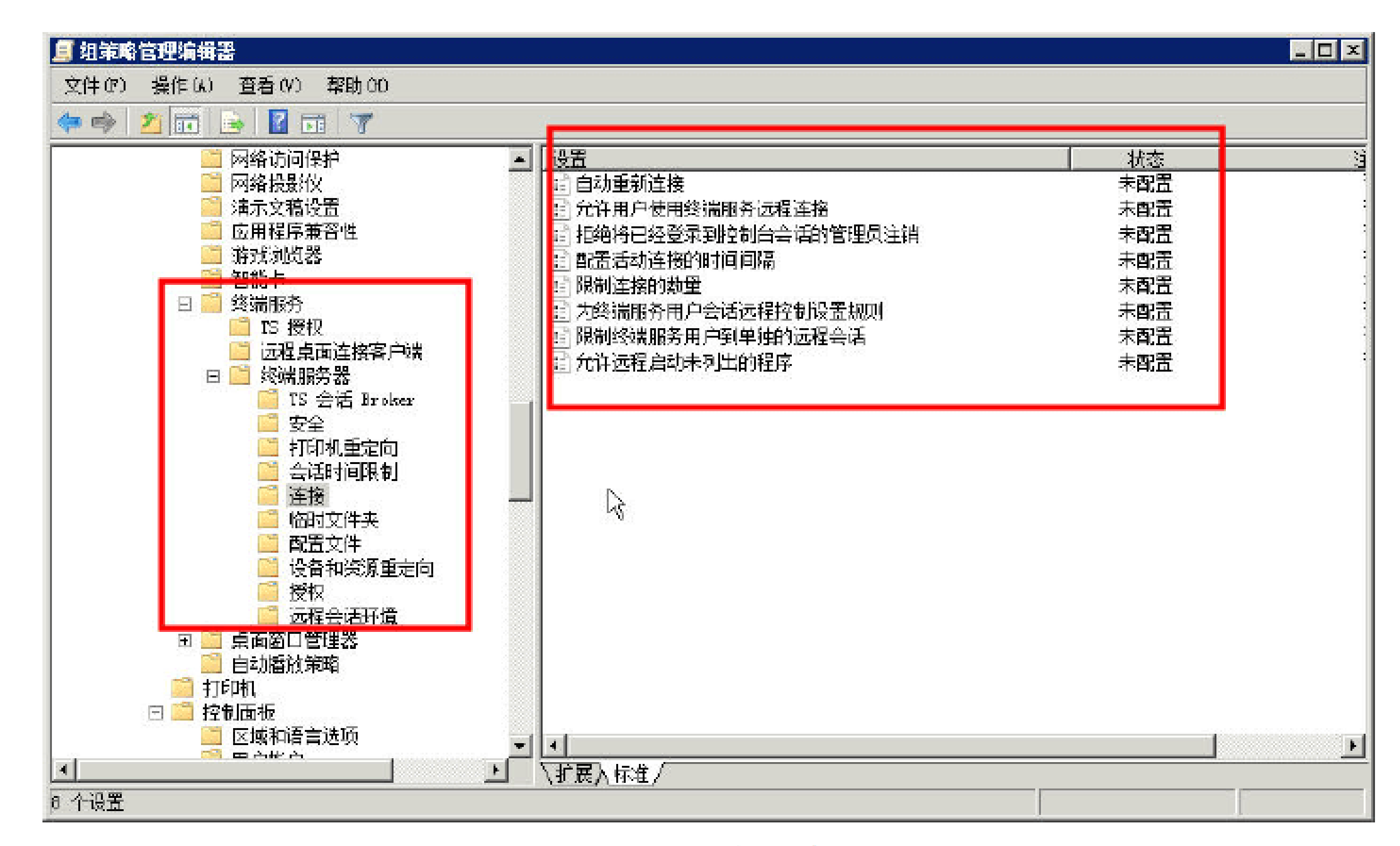


图 8-50　终端服务策略

该策略组可以配置终端服务的大多数设置，如图 8-51 所示。

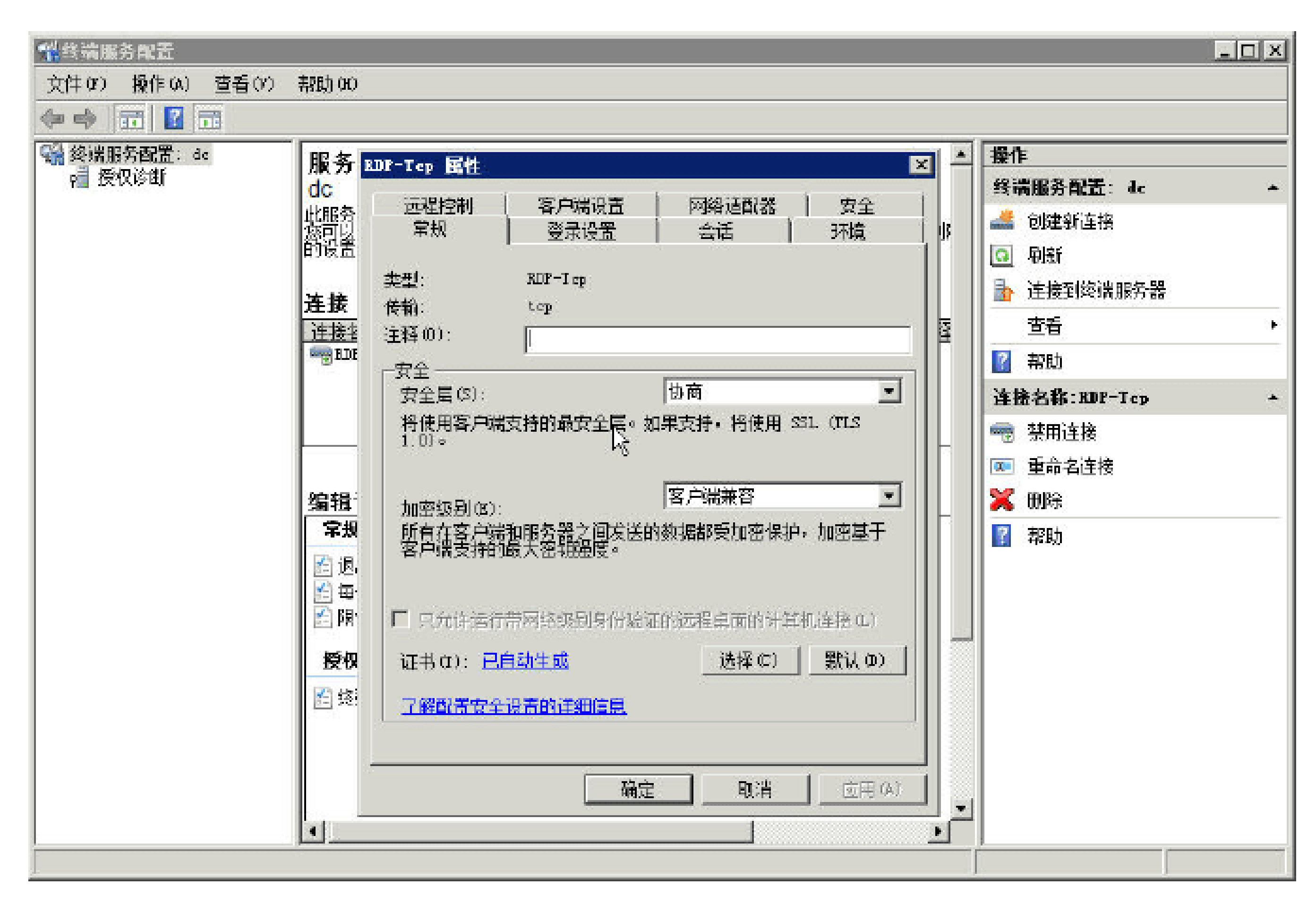


图 8-51　终端服务配置

8.3.7　系统配置策略

在“计算机配置→策略→管理模板→Windows 组件”中的“系统”策略组中，可以配置大多数的系统配置策略，例如“磁盘配额”、“登录”、“电源管理”、“关机选项”、“驱动程序安装”、“网络登录”等，还可以配置“激活‘关闭事件跟踪程序系统状态数据’功能”、“显示‘关闭事件跟踪程序’”、“在登录时不显示‘管理您的服务器’页”等，如图 8-52 所示。

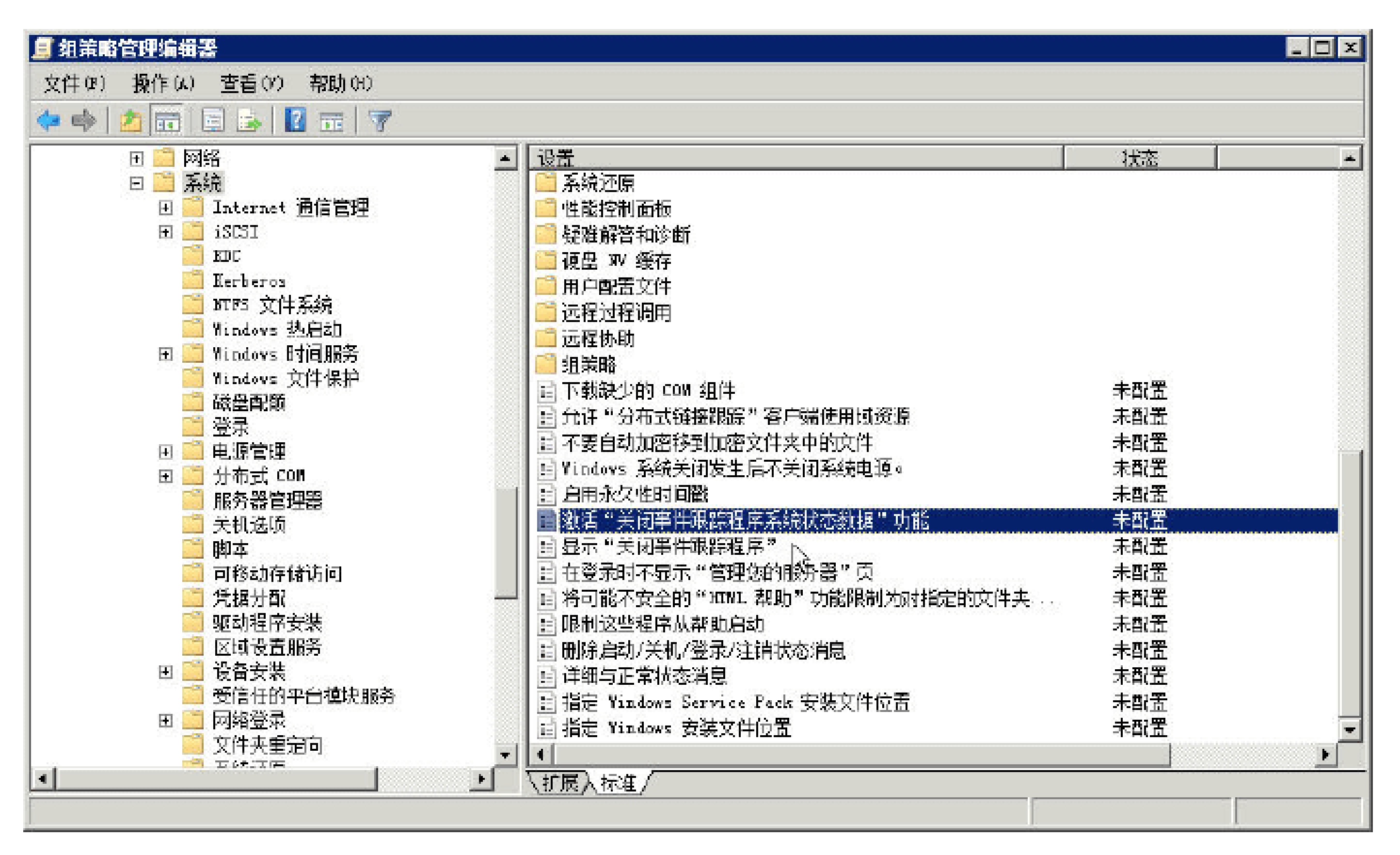


图 8-52　系统策略

8.3.8　文件夹重定向

用户设置和用户文件通常存储在位于“用户”文件夹下的本地用户配置文件中。本地用户配置文件中的文件只能从当前计算机进行访问，这样一来，使用多台计算机的用户就很难在多台计算机之间处理其数据并同步设置。现有两种不同的技术来解决该问题：“漫游配置文件”和“文件夹重定向”。这两种技术都有其各自的优点，可以单独使用，也可以结合起来使用，创建一种从一台计算机到另一台计算机的无缝用户体验。另外，它们还为管理用户数据的管理员提供了其他选项。

“文件夹重定向”允许管理员将文件夹的路径重定向到新位置。该位置可以是本地计算机上的一个文件夹，也可以是网络文件共享上的目录。用户能够使用服务器上的文档，如同该文档就在本地驱动器上一样。网络上任何计算机的用户都可使用该文件夹中的文档。

在“组策略管理编辑器”窗口中，定位到“用户配置→策略→Windows 设置→文件夹重定向”策略组中，可重定向的文件夹包括“AppDate（应用程序数据）”、“桌面”、“开始菜单”、“文档”、“图片”、“音乐”、“视频”、“收藏夹”、“联系人”、“下载”、“链接”、“搜索”及“保存的游戏”文件夹，如图 8-53 所示。

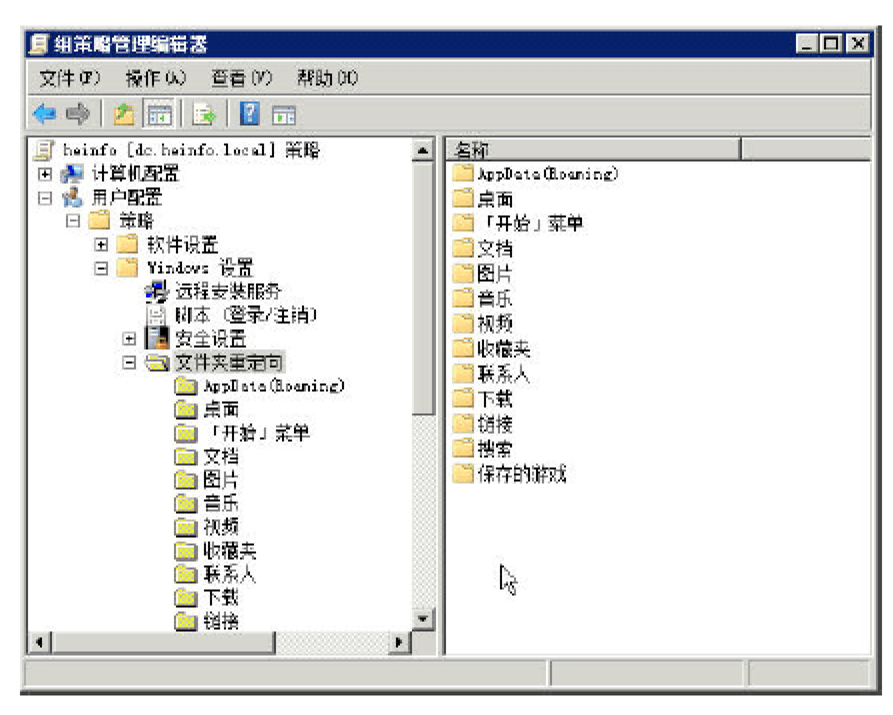


图 8-53　文件夹重定向

要使用“文件夹重定向”功能，必须将文件夹重定向到共享文件夹中，而不能重定向到本地路径。下面，以把该组织单位中的每个用户的文件夹重定向到“user-home”共享为例，介绍文件夹重定向的用法，步骤如下。

01 在服务器中找个剩余空间比较大的分区，在根目录创建 user-home 并创建共享，添加 Everyone 组为“共有者”权限，如图 8-54 所示。

02 在“文件夹重定向”中，右击“AppDate（Roming）”子文件夹，在弹出的快捷菜单中选择“属性”选项，如图 8-55 所示。

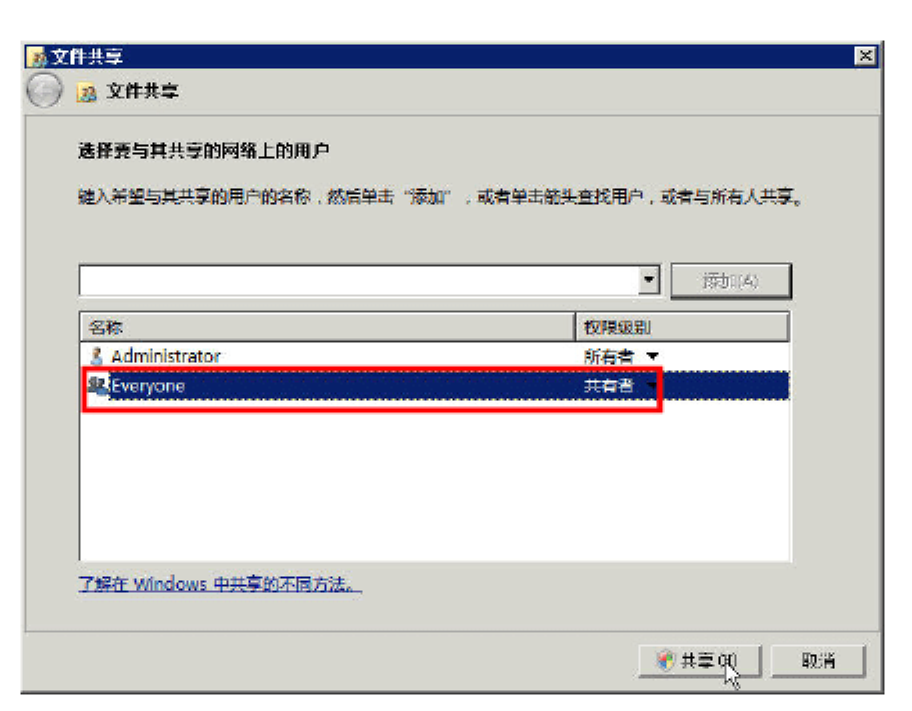


图 8-54　添加共享权限

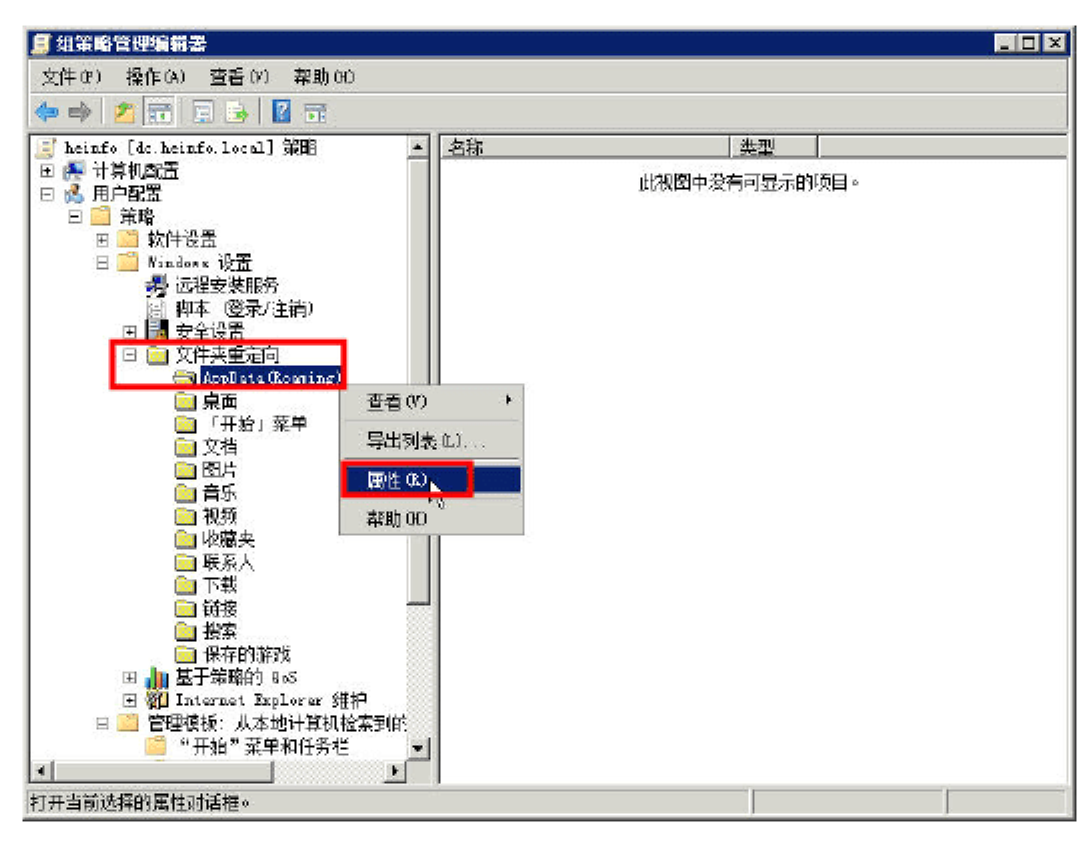


图 8-55　AppDate 属性

03 在“AppData（Roaming）属性”对话框，在“设置”下拉列表中选择“基本-将每个人的文件夹重定向到同一个位置”，在“目标文件夹设置”下拉列表中选择“在根目录路径下为每一用户创建一个文件夹”，然后在“根路径”文本框中输入图 8-54 中创建的共享，在本例中，该共享路径为\\dc.heinfo.local\user-home，如图 8-56 所示。这样，如果是 ws01 用户，该用户的 AppDate 文件夹将会被重重写到\\dc.heinfo.local\user-home\ws01\AppData\Roaming 目录。

04 在“设置”选项卡中，为 AppData（Roaming）选择重定向设置（推荐保存默认值），还可以配置“策略删除”设置（默认策略为“策略被删除时，将文件留在新位置”，即图 8-57 中设置的位置），如果选择“删除策略时将文件夹移回本地用户配置文件位置”选项，则该策略删除时，保存在服务器中的数据将会被移动到本地用户配置文件夹的位置。

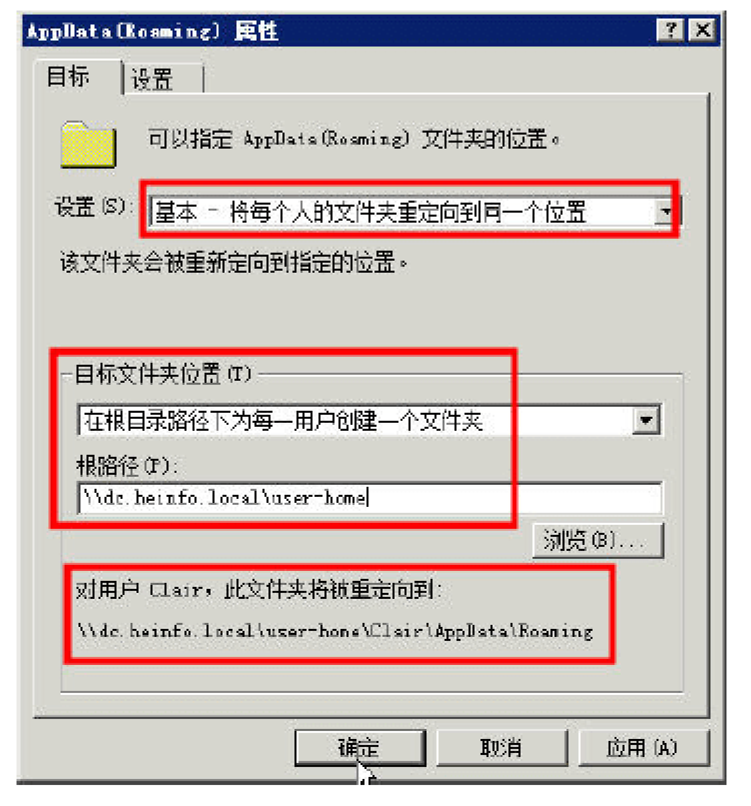


图 8-56　设置重定向文件夹的根路径

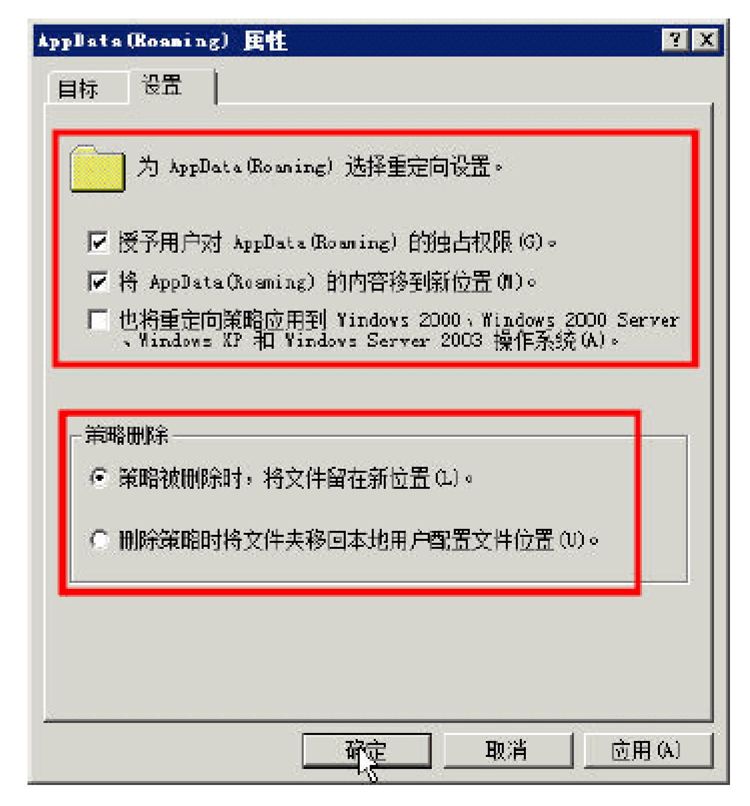


图 8-57　设置

05 在图 8-57 中单击“确定”按钮，弹出“警告”对话框，单击“是”按钮确认，如图 8-58 所示。

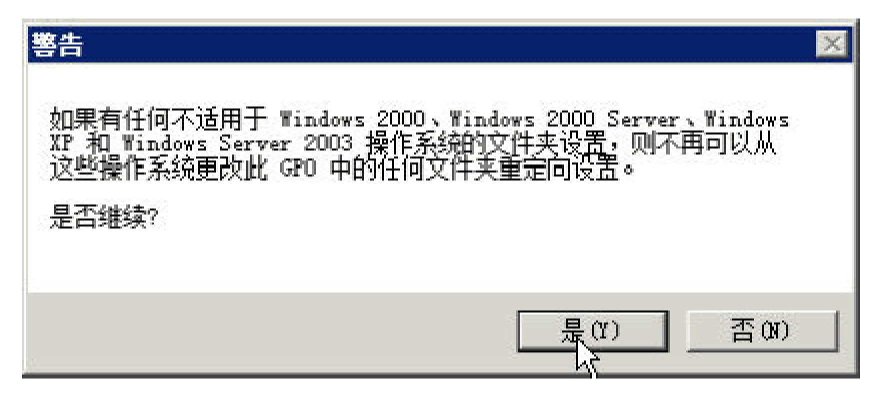


图 8-58　警告

06 请参照步骤 2～5 的设置，将“桌面”、“开始菜单”、“文档”、“图片”、“音乐”、“视频”、“收藏夹”、“联系人”、“下载”、“链接”等文件夹，重定向到同一位置即 \\dc.heinfo.local\user-home，其中“桌面”与“收藏夹”重定向设置时的截图如图 8-59、图 8-60 所示，其他的设置不一一介绍。

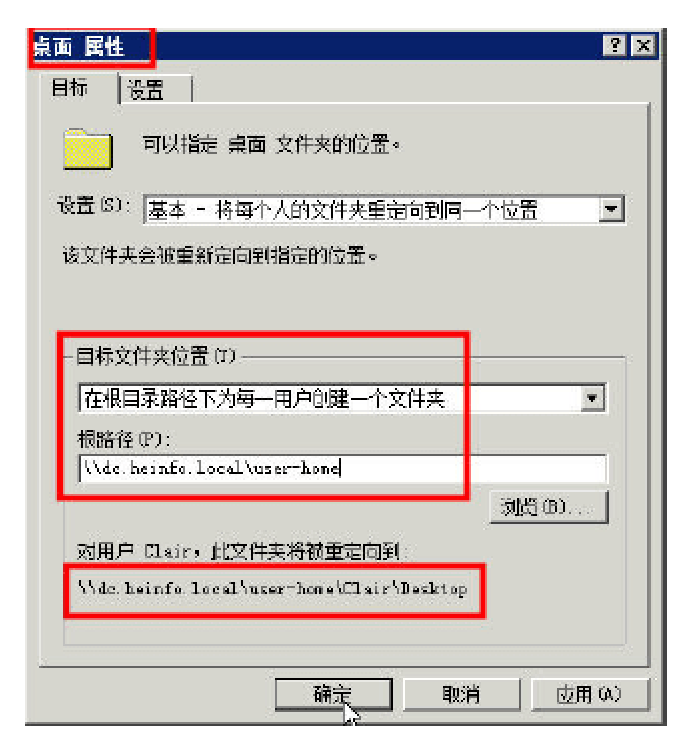


图 8-59　桌面文件夹重定向

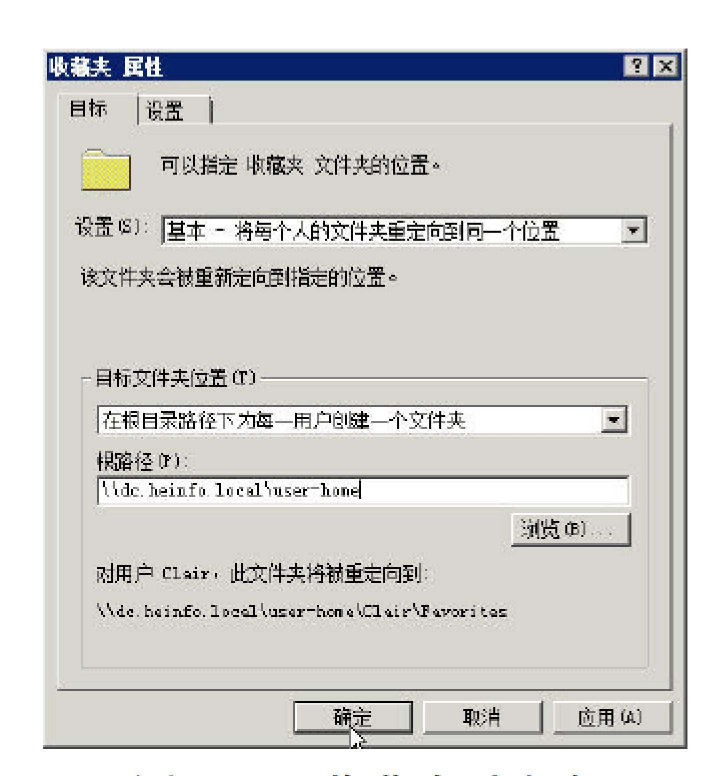


图 8-60　收藏夹重定向

8.3.9　用户配置中的 Internet Explorer 设置

在“用户配置”中的“Internet Explorer 维护”策略组中，包括“浏览器用户界面”、“连接”、“URL”、“安全”、“程序”5 部分，下面分别介绍。

01 在“用户配置→策略→Windows 设置→Internet Explorer 维护→浏览器用户界面”策略组中，包括“浏览器标题”、“自定义徽标和动画位图”、“浏览器工具栏自定义”3 部分。其中“浏览器标题”用来设置“Internet Explorer 浏览器标题”中出现的文字，如图 8-61 所示。

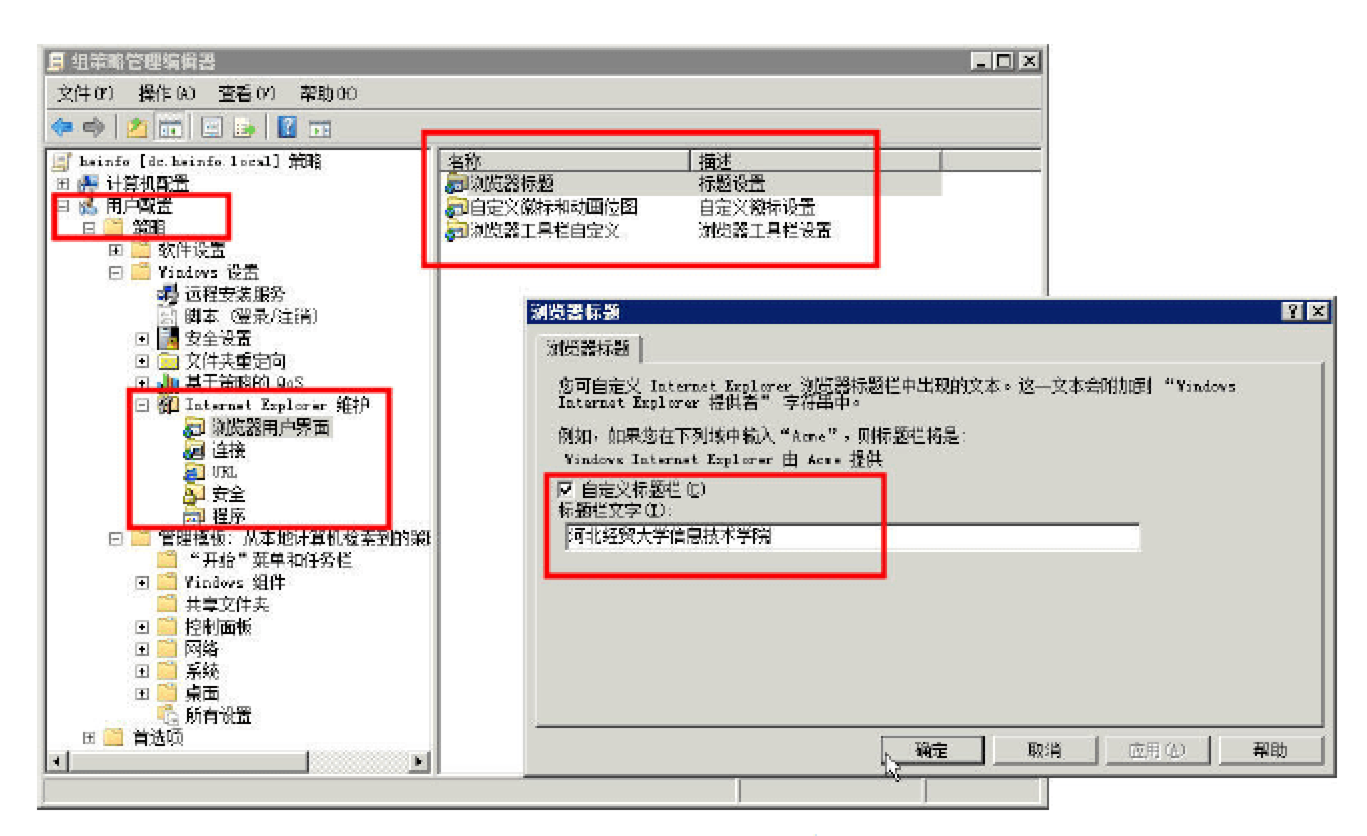


图 8-61　浏览器标题

02 在“自定义徽标和动画位图”处，设置 Internet Explorer 的静态徽标位图及 Internet Explorer 右上角的动画，如图 8-62 所示。

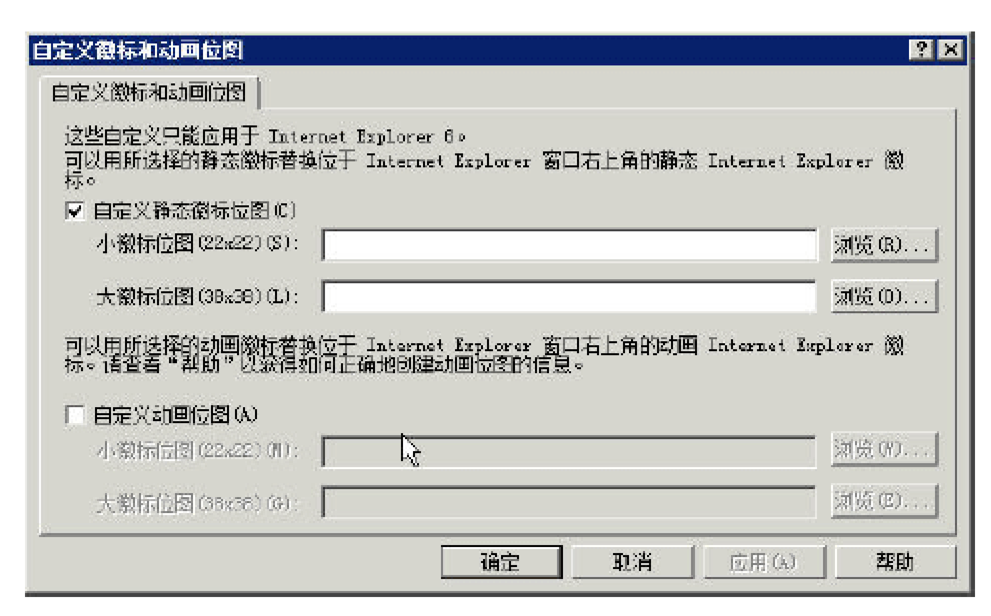


图 8-62　自定义徽标与动画



说 明

（1）这些自定义选项只能应用于 IE6。（2）在指定徽标与动画位置时，须使用网络路径共享文件夹及对应的位图与动画文件，而不是使用本地路径。

03 在“连接”选项中，用来指定“Internet Explorer”的“连接”选项卡中的设置，用户可以双击“连接设置”，在打开的“连接设置”对话框中，选中“从该计算机导入当前连接设置”单选按钮，单击“修改设置”按钮，打开“Internet”属性对话框，在“连接”选项卡中，设置“Internet 连接”、添加拨号和虚拟网络，单击“局域网设置”按钮，打开“局域网（LAN）设置”对话框，指定局域网设置等，如图 8-63 所示。

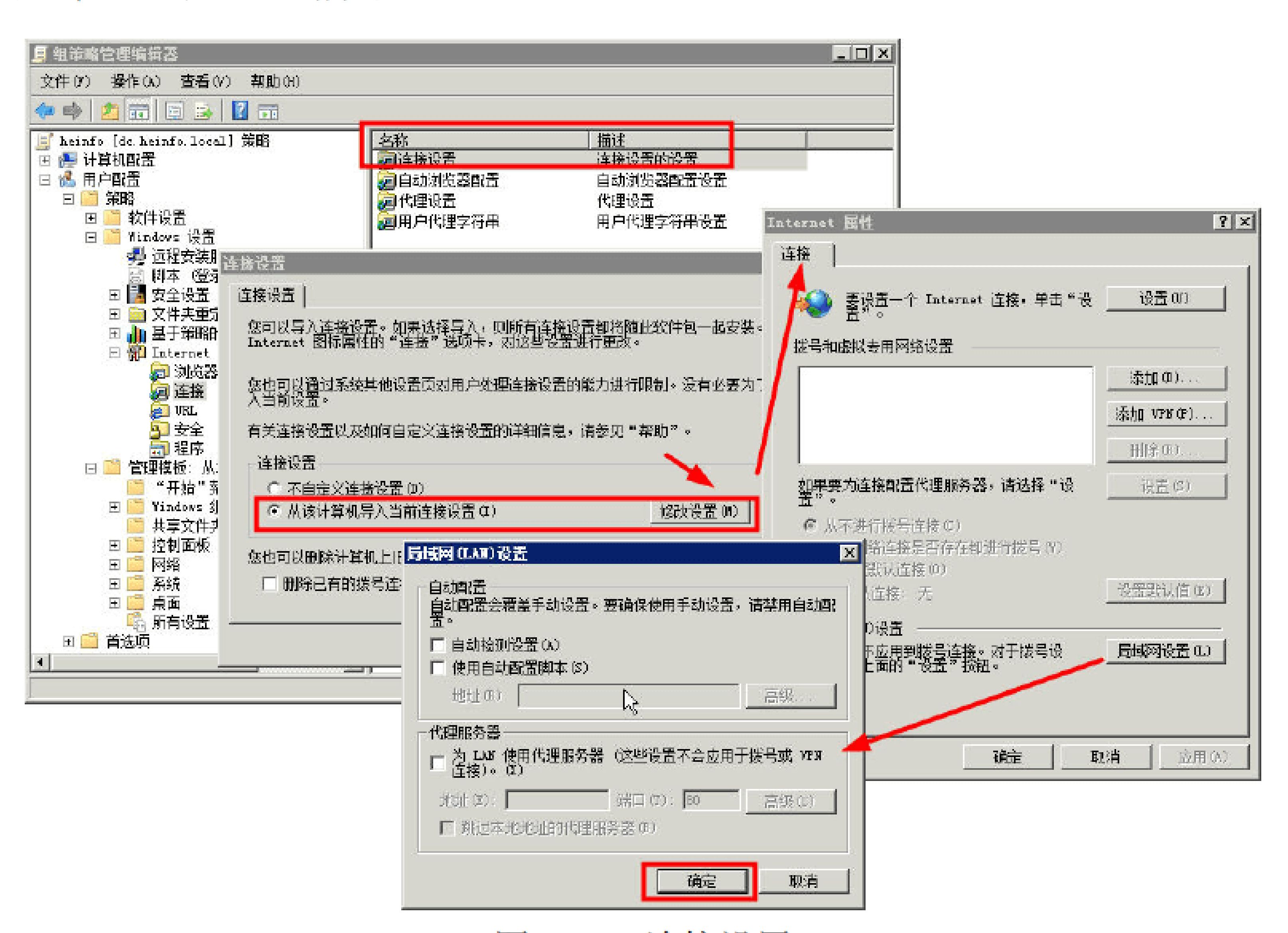


图 8-63　连接设置

04 在“URL”策略组中，可以指定 Internet Explorer 的“主页 URL”、“搜索栏 URL”、“联机支持页的 URL”等，如图 8-64 所示。

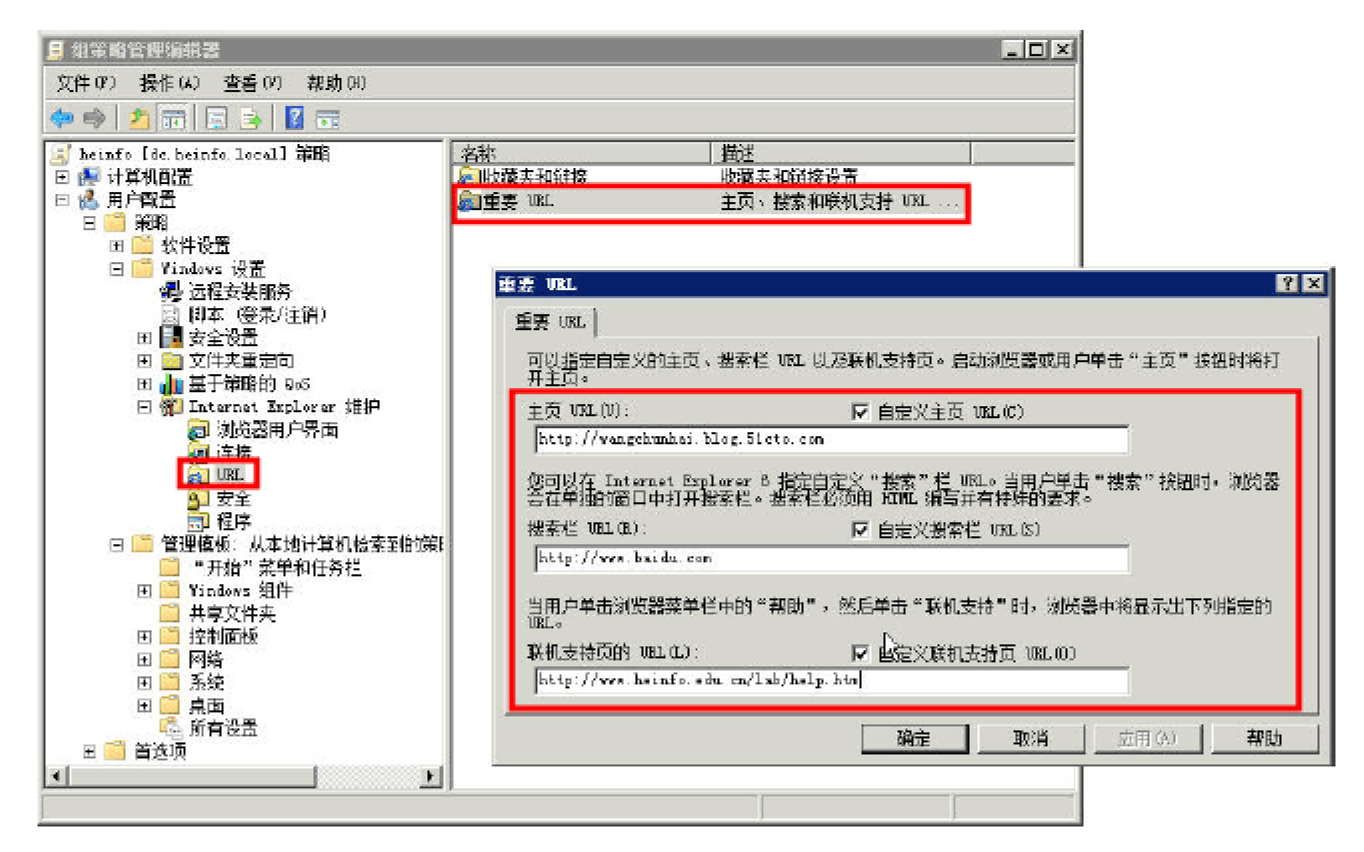


图 8-64 URL 设置

05 在“安全”策略组中，修改 Internet Explorer 的“安全”选项卡（如图 8-65 所示），在“Authenticode 设置”中，设置证书信息等。

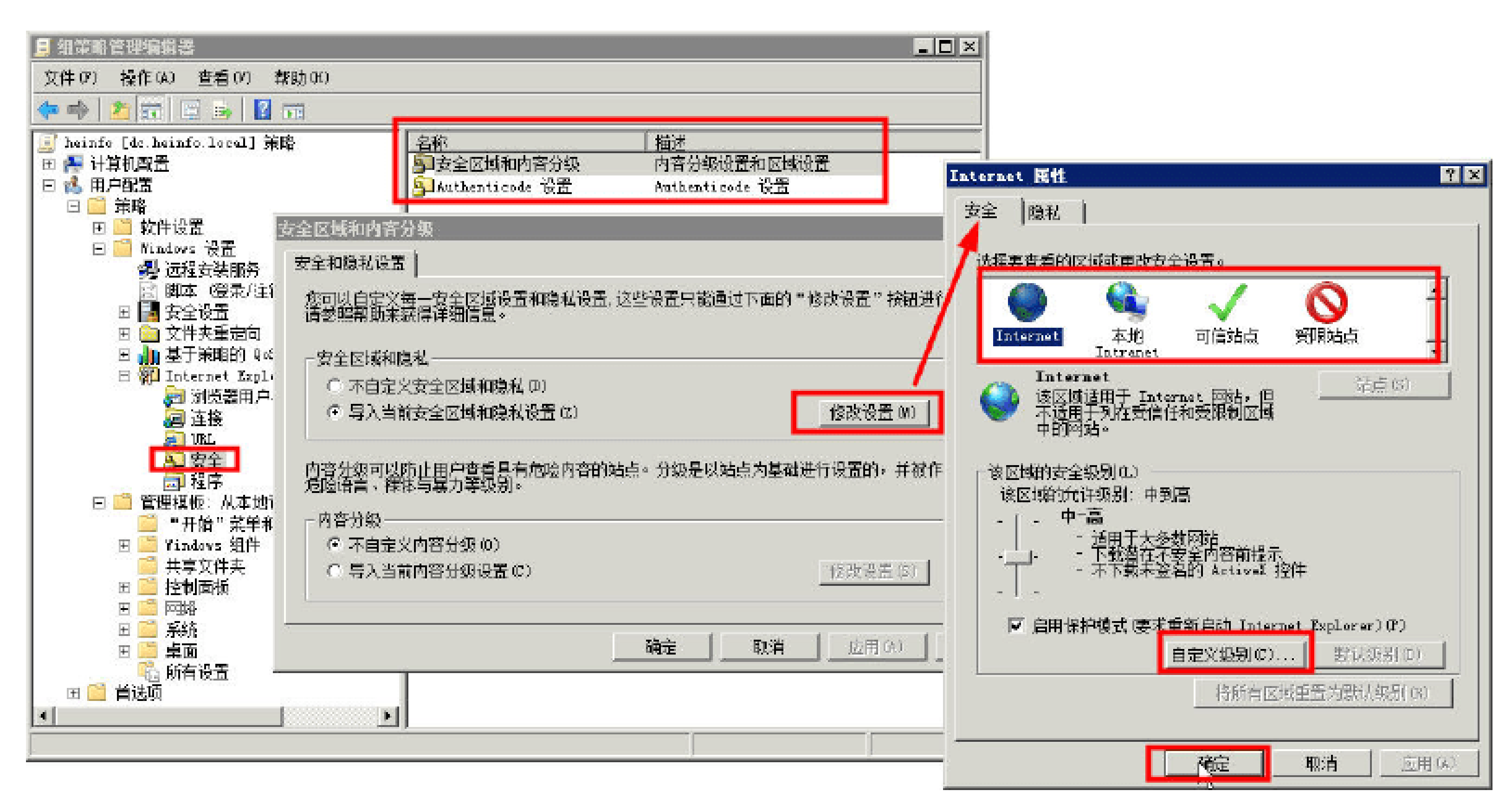


图 8-65 安全设置

06 在“程序”策略组中，用来修改 Internet Explorer 的“程序”选项卡中的设置，如图 8-66 所示。

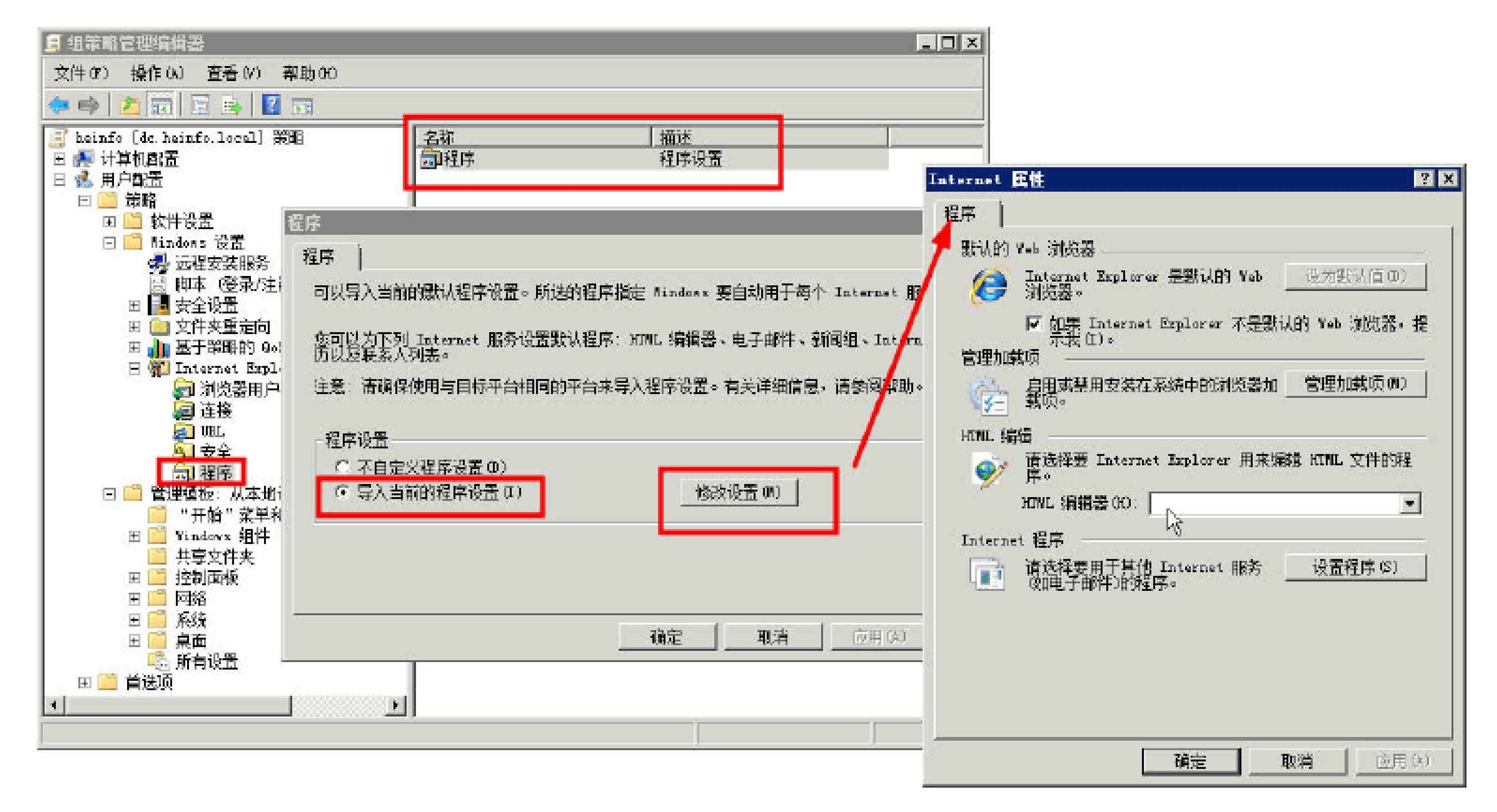


图 8-66 程序设置

8.3.10　开始菜单和任务栏

在“组策略管理编辑器”窗口中，定位到“用户配置→策略→管理模板→开始菜单和任务栏”策略组，可以配置开始菜单和任务栏中显示或加载的菜单项，如图 8-67 所示。

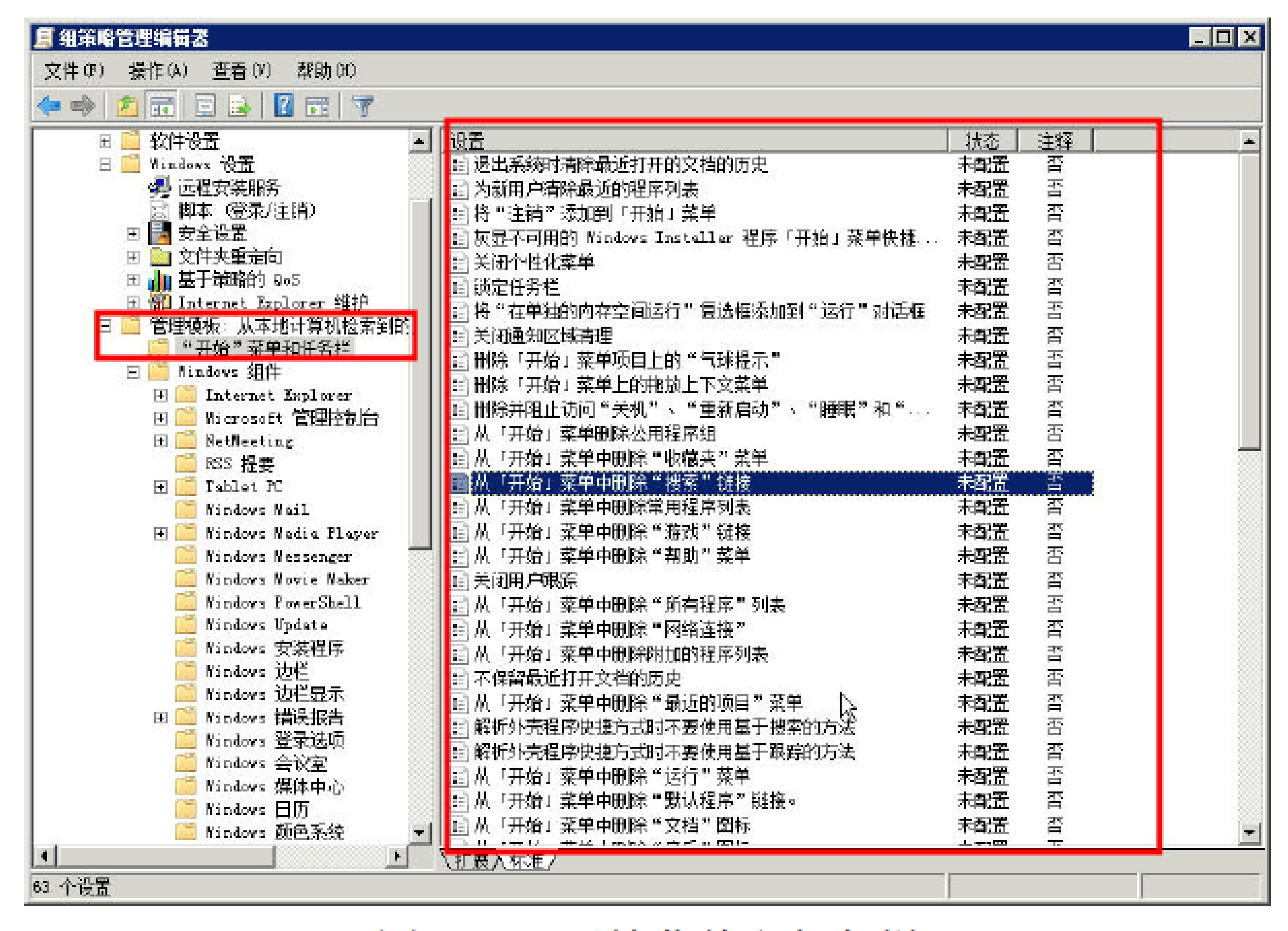


图 8-67　开始菜单和任务栏

8.4　首　选　项

使用组策略管理控制台，可以在编辑任何基于域的组策略对象时配置首选项。“首选项”节点显示在“计算机配置”和“用户配置”下。编辑器在以下两个类别下显示首选项扩展：“Windows 设置”和“控制面板设置”。

“Windows 设置”下的首选项扩展包括：

- 应用程序扩展：配置应用程序的设置。
- 驱动器映射扩展：创建、修改或删除驱动器映射并配置所有驱动器的可见性。
- 环境扩展：创建、修改或删除环境变量。
- 文件扩展：复制、修改文件的属性，以及替换或删除文件。
- 文件夹扩展：创建、修改或删除文件夹。
- InI 文件扩展：添加、替换或删除配置设置（.ini）或安装信息（.inf）文件中的段或属性。
- 网络共享扩展：创建、修改或删除（“取消共享”）共享。
- 注册表扩展：复制注册表设置并将其应用到其他计算机。创建、替换或删除注册表设置。
- 快捷方式扩展：创建、修改或删除快捷方式。

“控制面板设置”下的首选项扩展包括：

- 数据源扩展：创建、修改或删除开放式数据库连接（ODBC）数据源名称。
- 设备扩展：启用或禁用硬件设备或设备的类。

- 文件夹选项扩展：配置文件夹选项；创建、修改或删除文件扩展名的“打开方式”关联；创建、修改或删除与文件类型关联的文件扩展名。
- Internet 设置扩展：修改用户可配置的 Internet 设置。
- 本地用户和组扩展：创建、修改或删除本地用户和组。
- 网络选项扩展：创建、修改或删除虚拟专用网络（VPN）或拨号网络（DUN）连接。
- 电源选项扩展：修改电源选项以及创建、修改或删除电源方案。
- 打印机扩展：创建、修改或删除 TCP/IP、共享和本地打印机连接。
- 区域选项扩展：修改区域选项。
- 计划任务扩展：创建、修改或删除计划任务或即时任务。
- 服务扩展：修改服务。
- 开始菜单扩展：修改“开始”菜单选项。

8.4.1 驱动器映射首选项

组策略包括驱动器映射首选项扩展。对于用户，使用该扩展可以：

- 创建到网络共享的动态驱动器映射。
- 使用备用的用户凭据创建到网络共享的动态驱动器映射。
- 修改映射的驱动器及其属性。
- 删除单个映射的驱动器。
- 删除所有映射的驱动器或从前面指定的驱动器号中删除所有映射的驱动器。
- 隐藏或显示单个驱动器或所有驱动器，包括映射的驱动器和物理驱动器。

接下来通过具体的实例，介绍驱动器首选项的配置方法，步骤如下。

01 在服务器的 E 盘创建一个文件夹并启用共享，例如创建的文件夹名为 software，如图 8-68 所示。

02 设置共享权限 “Administrator”为“所有者”，添加“Everyone”为“读者”，并在该文件夹中复制一些程序，如图 8-69 所示。

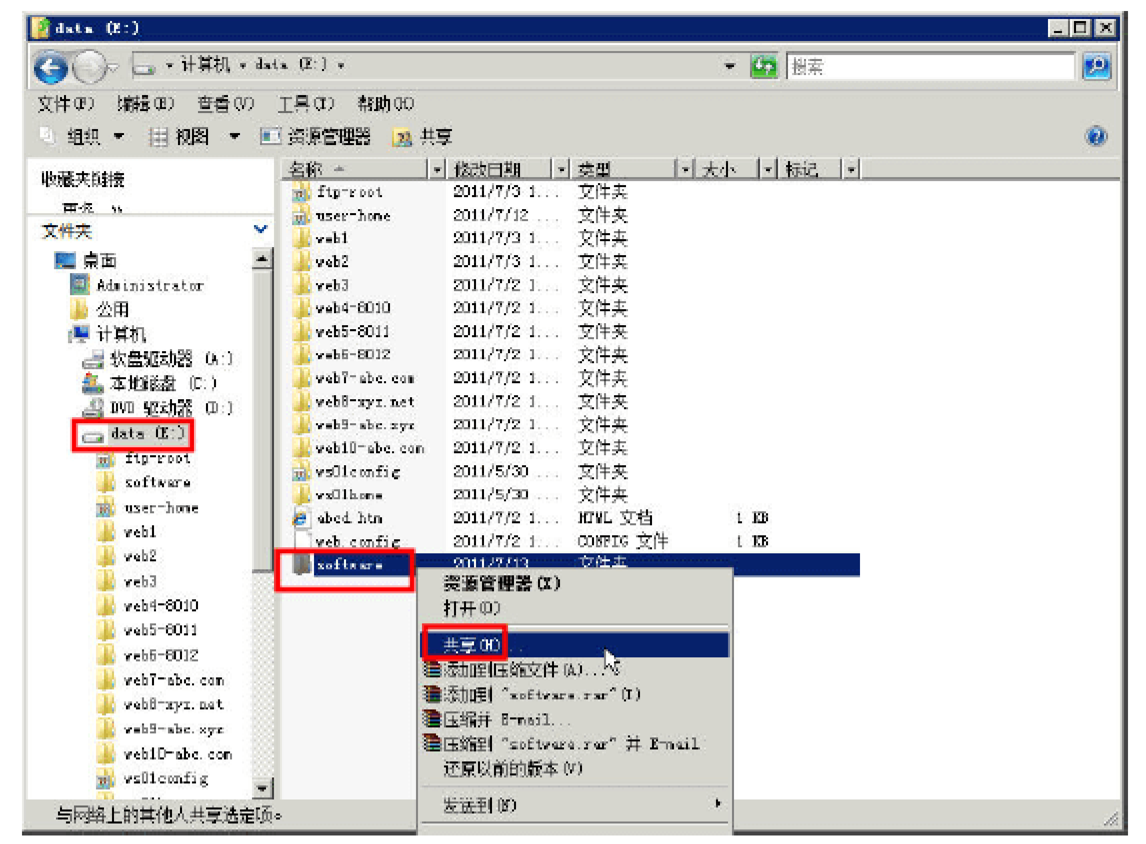


图 8-68 创建文件夹并启用共享

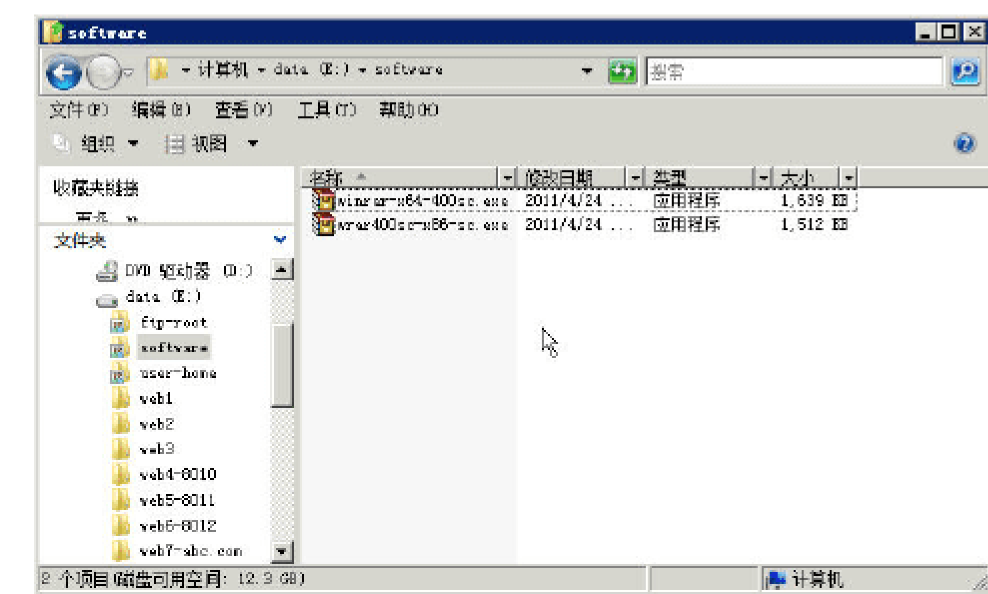


图 8-69 向文件夹复制一些程序

03 在“组策略管理编辑器”窗口中，定位到“用户配置→首选项→驱动器映射”，在右侧的空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→映射驱动器”选项，如图 8-70 所示。

04 在弹出的“新驱动器 属性”对话框中，在“操作”下接列表中选择“更新”选项，在“位置”文本框中输入要连接的服务器共享。在本例中，输入\\dc.heinfo.local\software（这是图 8-68 中创建的共享，而 dc.heinfo.local 是该服务器的名称），在“驱动器号”选项组处选择“使用”，并在下拉列表中选择一个盘符，如本例选择 X，如图 8-71 所示。

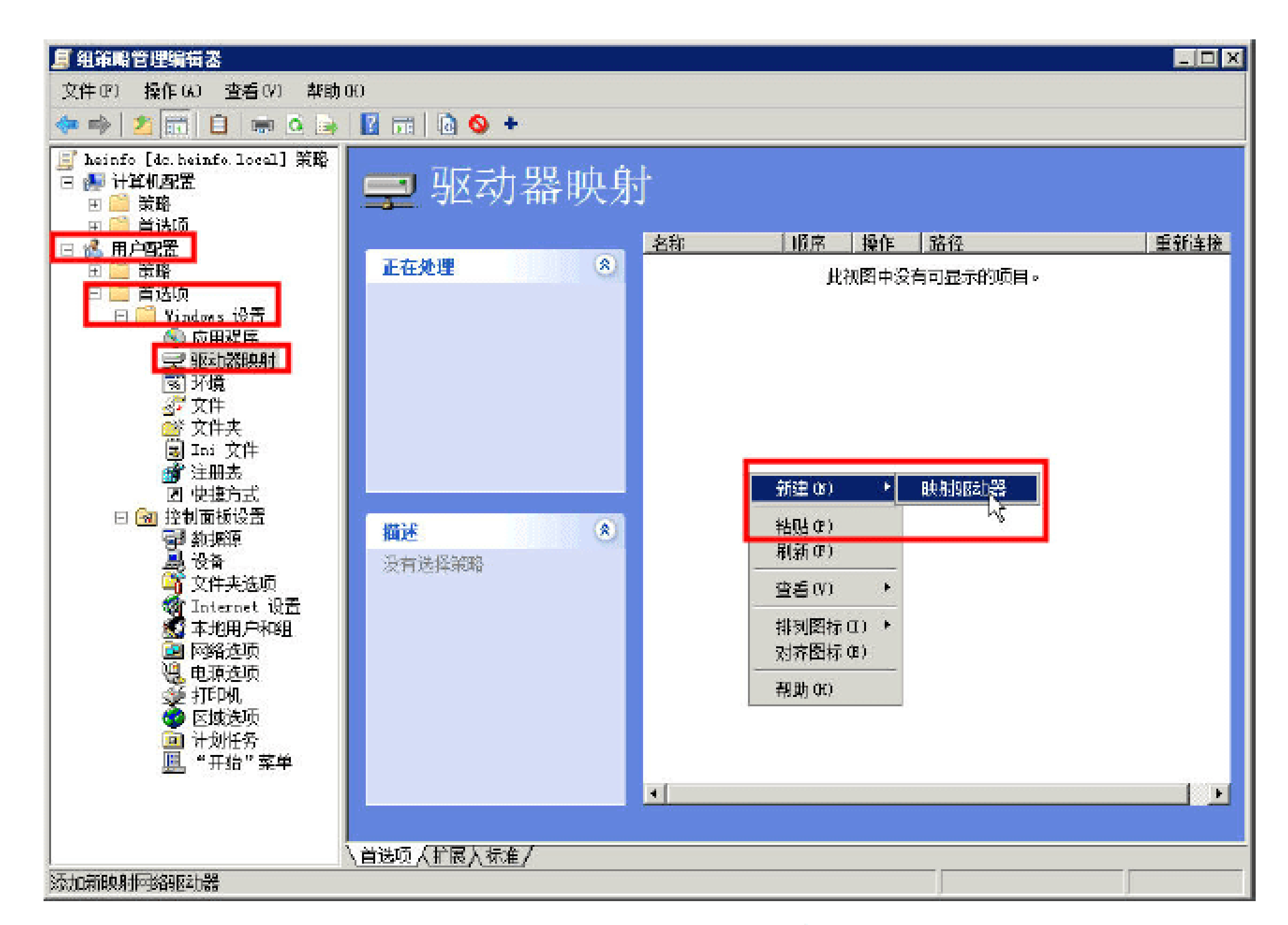


图 8-70　新建映射驱动器

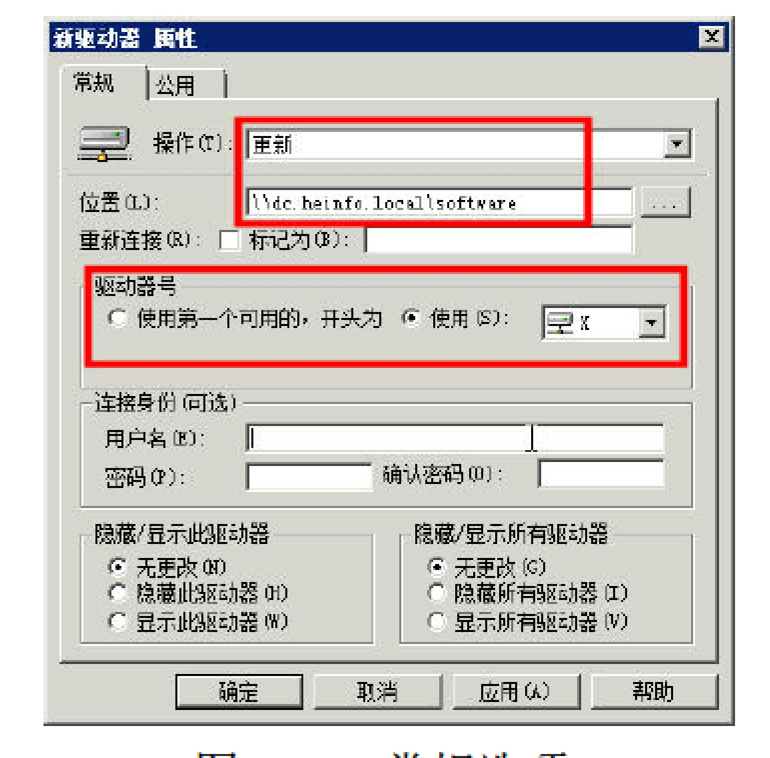
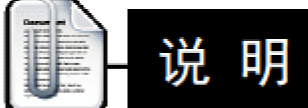


图 8-71　常规选项



说 明

在“首选项”中，在“常规”选项卡中的“操作”功能包括 4 个操作选项：创建、替换、更新和删除。各操作意义如下：

- 创建：为用户创建新的映射驱动器。
- 删除：删除用户的映射驱动器。
- 替换：删除并重新创建用户的映射驱动器。“替换”操作的最终结果是覆盖与映射驱动器相关的所有现有设置。如果驱动器映射不存在，则“替换”操作会创建新的驱动器映射。
- 更新：修改用户的现有映射驱动器的设置。该操作与“替换”不同，它仅更新在该首选项中定义的设置。所有其他设置保持为在映射驱动器上配置的状态。如果驱动器映射不存在，则“更新”操作会创建新的驱动器映射。

在使用其他“首选项”的“操作”功能时，通常也会包括创建、替换、更新和删除 4 个选项，各意义与上述类似。

05 在“公用”选项卡中，设置了所有项目共同的选项，如图 8-72 所示。

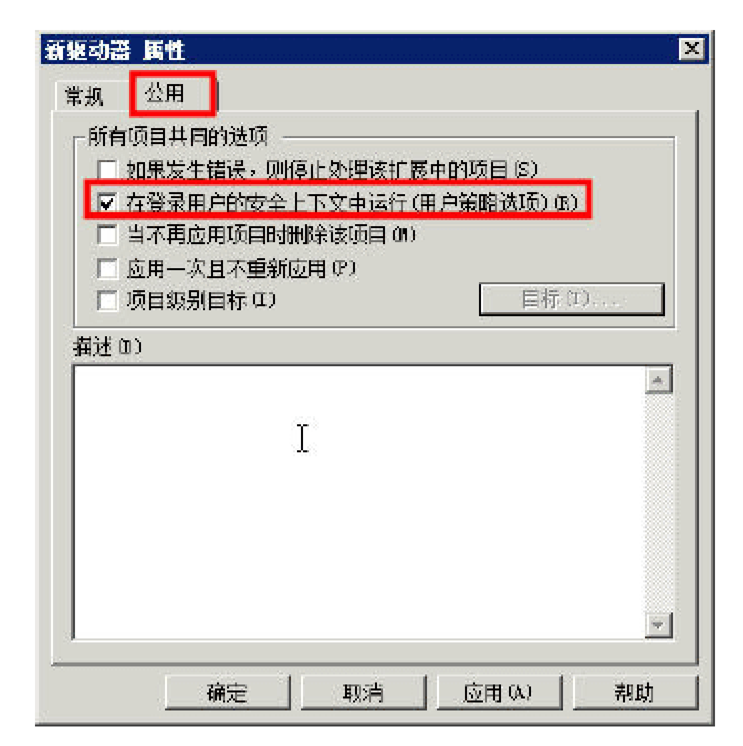


图 8-72 公用选项

各选项意义如下：

- 如果发生错误，则停止处理该扩展中的项目：在默认情况下，失败的首选项不阻止处理同一扩展中的其他首选项。如果选择了“如果发生错误，则停止处理该扩展中的项目”选项，则失败的首选项会阻止处理扩展中的剩余首选项。此更改行为限于主持的组策略对象（GPO），不扩展到其他 GPO。首选扩展从列表的底部开始处理首选项，一直到列表的顶部。在失败的首选项得到应用之前，会成功应用各首选项。首选扩展只停止处理失败首选项之后的首选项。
- 在登录用户的安全上下文中运行（用户策略选项）：组策略在两种安全上下文中应用用户首选项，系统账户和登录用户。 在默认情况下，组策略使用系统账户的安全上下文处理用户首选项。在此安全上下文中，首选扩展仅可用于该计算机的环境变量和系统资源。 如果选择了“在登录用户的安全上下文中运行”选项，将更改在其下处理首选项的安全上下文。首选扩展在登录用户的安全上下文中处理首选项，这允许首选扩展以用户而不是计算机形式访问资源。当使用计算机可能没有权限访问资源的驱动器映射或其他首选项，或使用环境变量时，这尤其重要。在非登录用户的安全上下文中评估时，许多环境变量的值会有所不同。
- 当不再应用项目时删除该项目：组策略将策略设置和首选项应用于用户和计算机。通过将一个或多个组策略对象（GPO）链接到 Active Directory 站点、域或组织单位，可确定哪些用户和计算机接收这些项目。驻留在这些容器中的用户和计算机对象，接收链接的 GPO 中定义的策略设置和首选项，因为它们在 GPO 的作用域之内。 与策略设置不同，默认情况下，主持的 GPO 超出用户和计算机作用域时首选项不会被删除。如果选择了“当不再应用项目时删除该项目”选项，将更改此行为。选择此选项之后，首选扩展确定首选项是否应用于目标用户或计算机（作用域之外）。如果首选扩展确定首选项超出作用域，它将删除与首选项相关的设置。如果选择此选项将操作更改为“替换”。在组策略应用期间，首选扩展重新创建（删除并创建）首选项的结果。当首选项超出用户或计算机的作用域时，首选项的结果被删除，但不会重新创建。通过使用项目级目标或更高级组策略筛选器（如 WMI 和安全组筛选器），可以使首选项超出作用域。 当首选项操作设置为“删除”时，“当不再应用项目时删除该项目”选项不可用。

- 应用一次且不重复应用：默认情况下，组策略每次刷新时都重写首选项的结果。这样可确保首选项的结果与管理员在组策略对象中的指定保持一致。 如果选择了“应用一次且不重复应用”选项，将更改此行为，因为首选扩展将首选项的结果应用于用户或计算机的次数仅为一次。当用户不想重复应用首选项的结果时，此选项非常有用。
- 项目级目标：可以使用项目级目标来更改个别首选项的作用域，使首选项仅应用于选定的用户或计算机。可以在单个组策略对象（GPO）中包括多个首选项，每个首选项都针对选定的用户或计算机进行了自定义，并且仅将设置应用于相关用户或计算机。每个目标项都将导致一个 true 或 false 值。可以将多个目标项应用于首选项，并选择逻辑运算（AND 或 OR），通过逻辑运算将每个目标项与前一目标项相组合。如果首选项的所有目标项的组合值为 false，则首选项中的设置不应用于用户或计算机。使用目标集合，还可以创建插入语句。

06 在图 8-72 中，选中“项目级别目标”，然后单击“目标”按钮，弹出“目标编辑器”对话框，单击“新建项目”，可以看出有多个项目供选择，如图 8-73 所示。

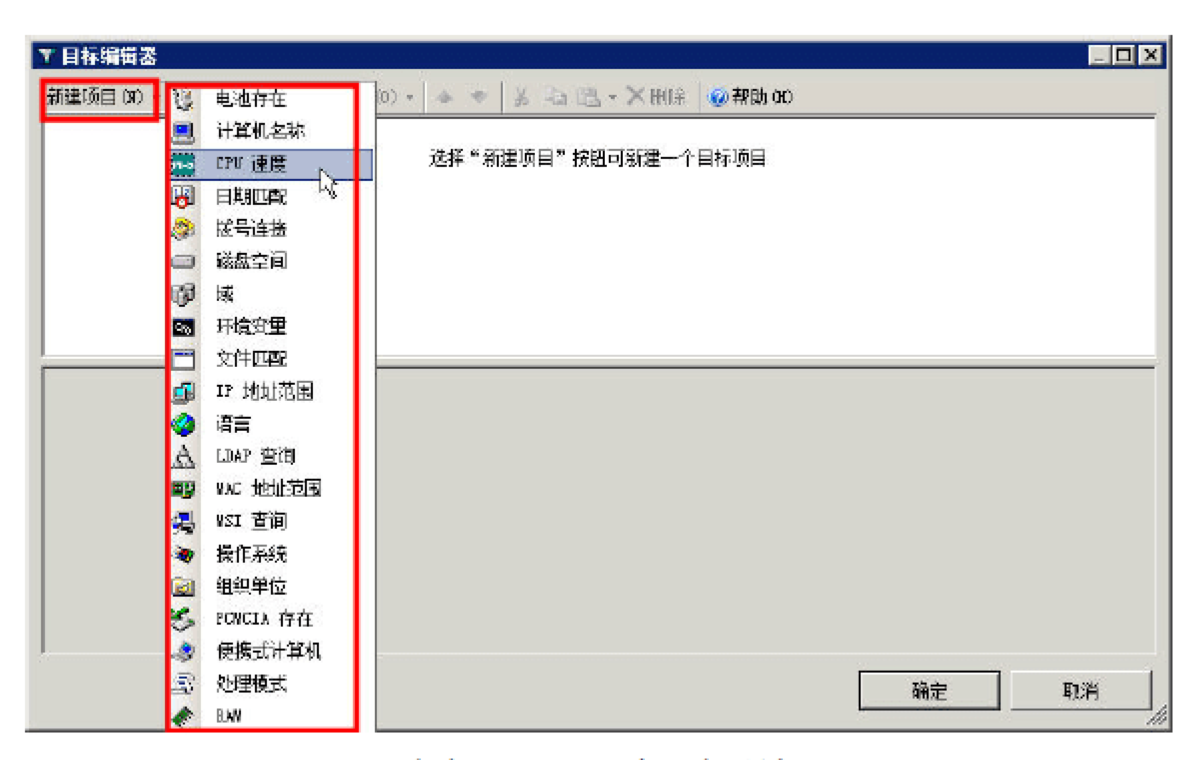


图 8-73 项目级别

在图 8-73 中，可以通过新建项目来确定现有首选项，使其仅应用于特定用户或计算机，例如选择“CPU 速度”选项，可以设置 CPU 的速度大于或等于某一频率，如果选择“操作系统”选项，则可以选择操作系统的版本（如 Windows XP、Windows Vista 等），如图 8-74 所示。

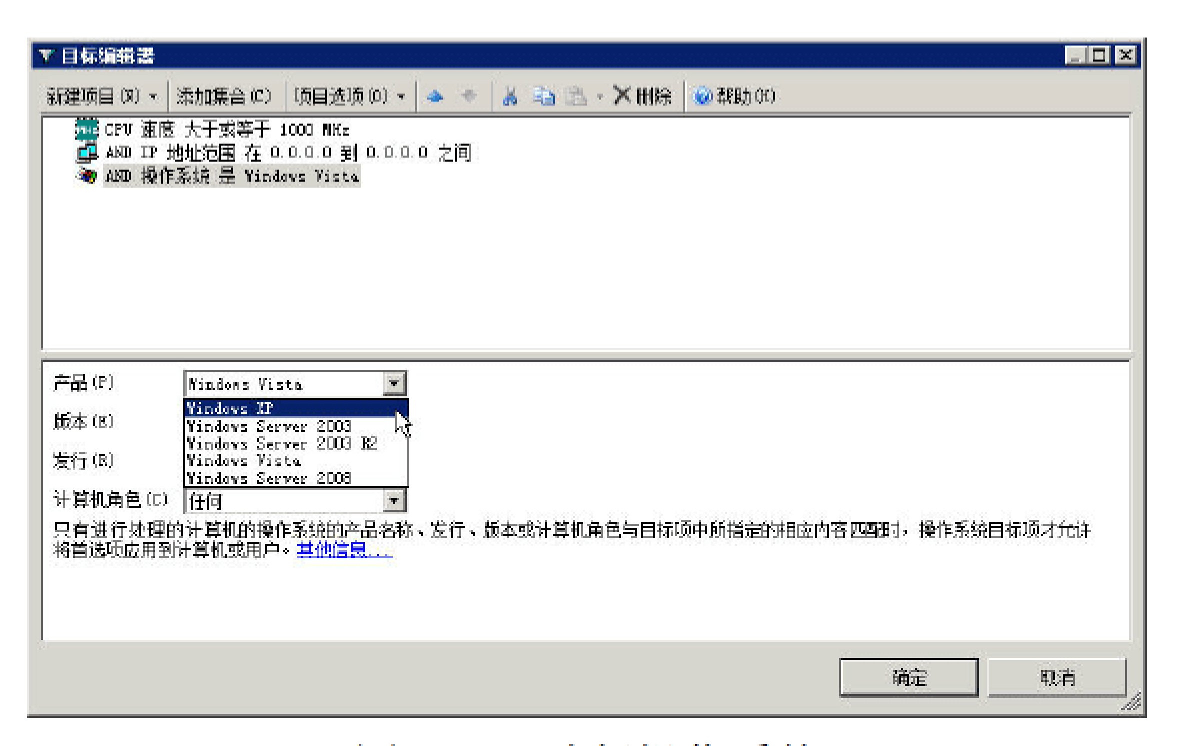


图 8-74 选择操作系统

当创建多个项目时，可以打开“项目选项”菜单，设置项目之间的关系（和、或、是、不是）

等，如图 8-75 所示。

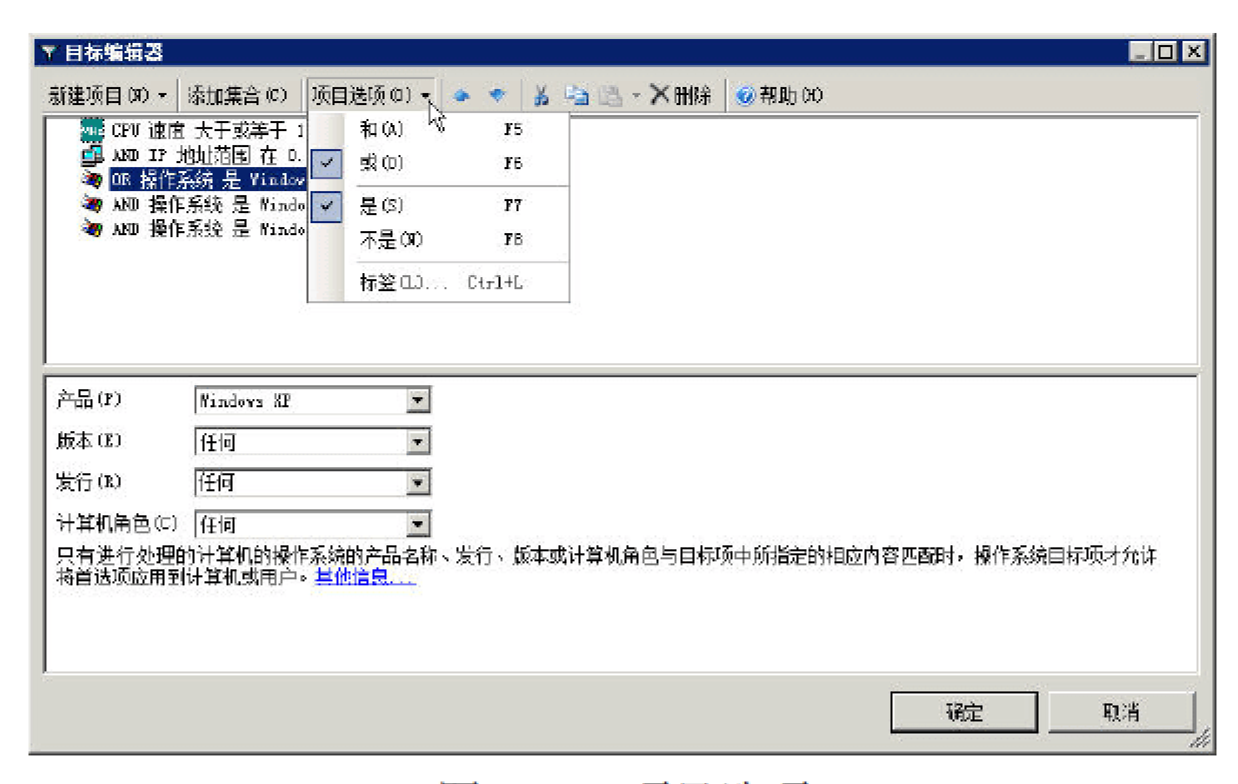


图 8-75 项目选项

通过目标编辑器，你可以设置 CPU、IP 地址、操作系统、磁盘空间、组织单位等选项，来确定应用首选项的目标。请大家根据自己的需要选择。

8.4.2 环境首选项

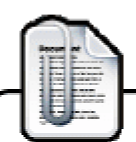
组策略包括环境首选项扩展。对于计算机或用户，使用此扩展可以：

- 创建永久性用户或系统环境变量。
- 修改环境变量。例如：
  - 修改命令提示符（方法是修改 PROMPT 系统变量）。
  - 修改 TEMP 文件夹的位置（方法是修改 TEMP 系统变量）。
  - 替换整个 PATH 变量的值。
  - 将分号分隔的段添加到 PATH 变量。
  - 将分号分隔的段从 PATH 变量中删除。
  - 更改 PATH 变量的分号分隔的段的文本大小写。
- 删除环境变量。

下面通过具体的实例，介绍环境首选项的使用，步骤如下。

01 定位到“首选项→Windows 设置→环境”，在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→环境变量”选项，如图 8-76 所示。

02 在“新环境 属性”对话框中，在“操作”下拉列表中选择“更新”选项，选中“用户变量”单选按钮，在“名称”文本框中输入 TEMP，在“值”文本框处设置 c:\temp，如图 8-77 所示。这样，将把用户的临时目录更改为 c:\temp。



说 明

用户可以创建不存在的环境变量，也可以“更新”或“删除”已经存在的环境变量。

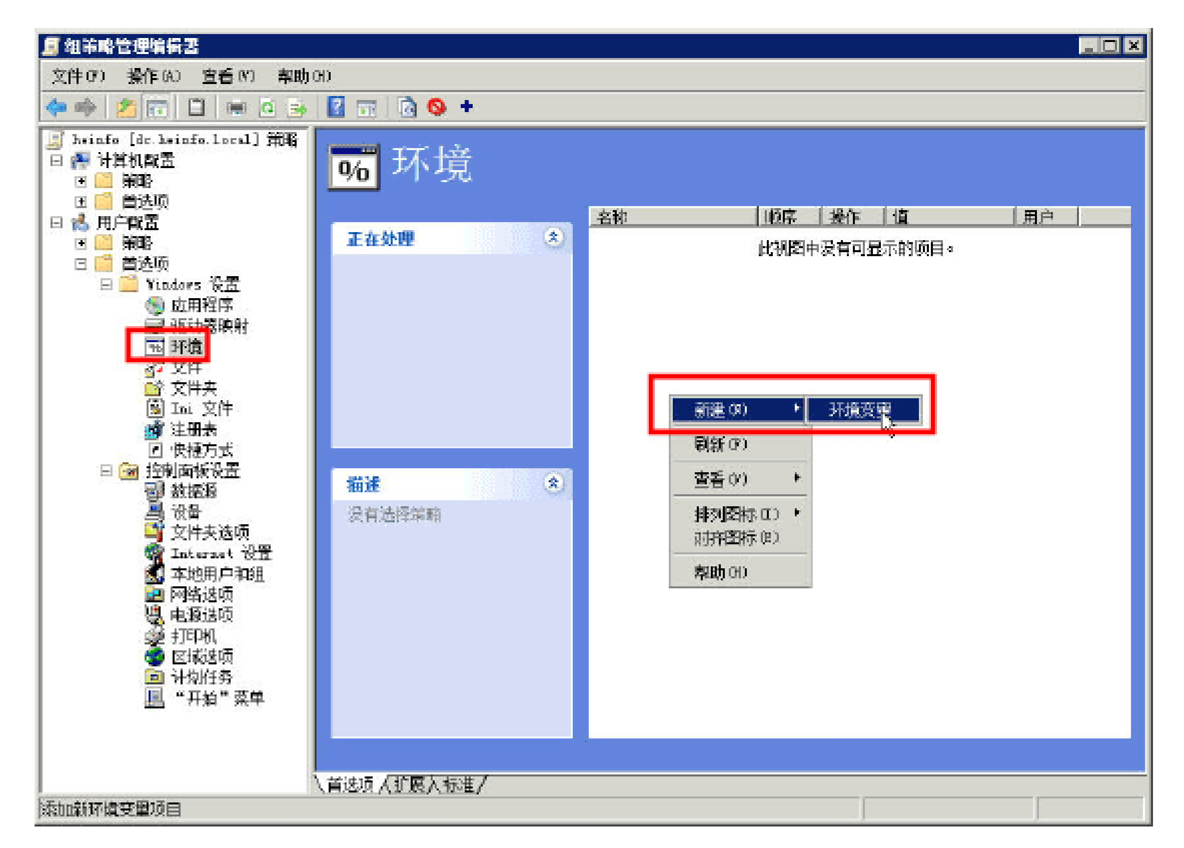




图 8-76　新建环境变量

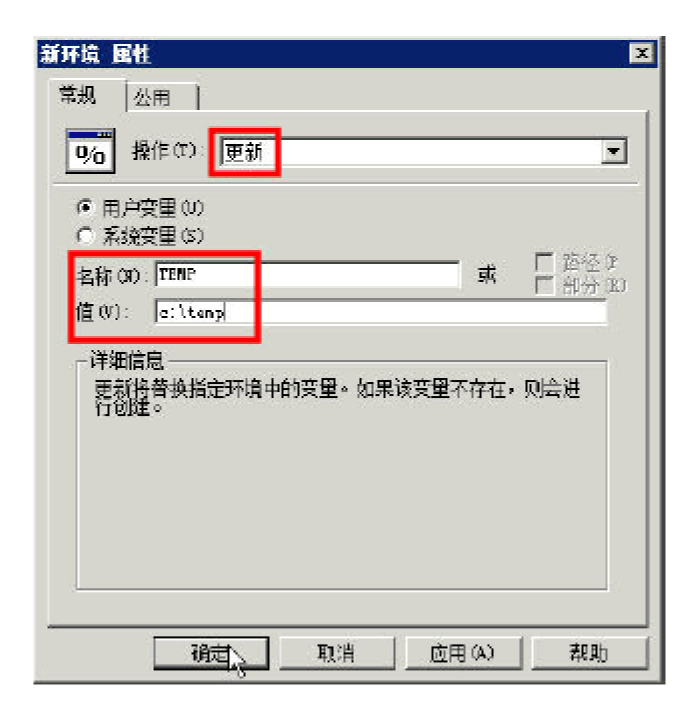


图 8-77　新环境属性

如果要查看系统可用的环境变量，可以打开“系统属性→高级”选项卡，单击“环境变量”按钮，会弹出“环境变量”对话框，显示“用户变量”及“系统变量”，如图 8-78 所示。

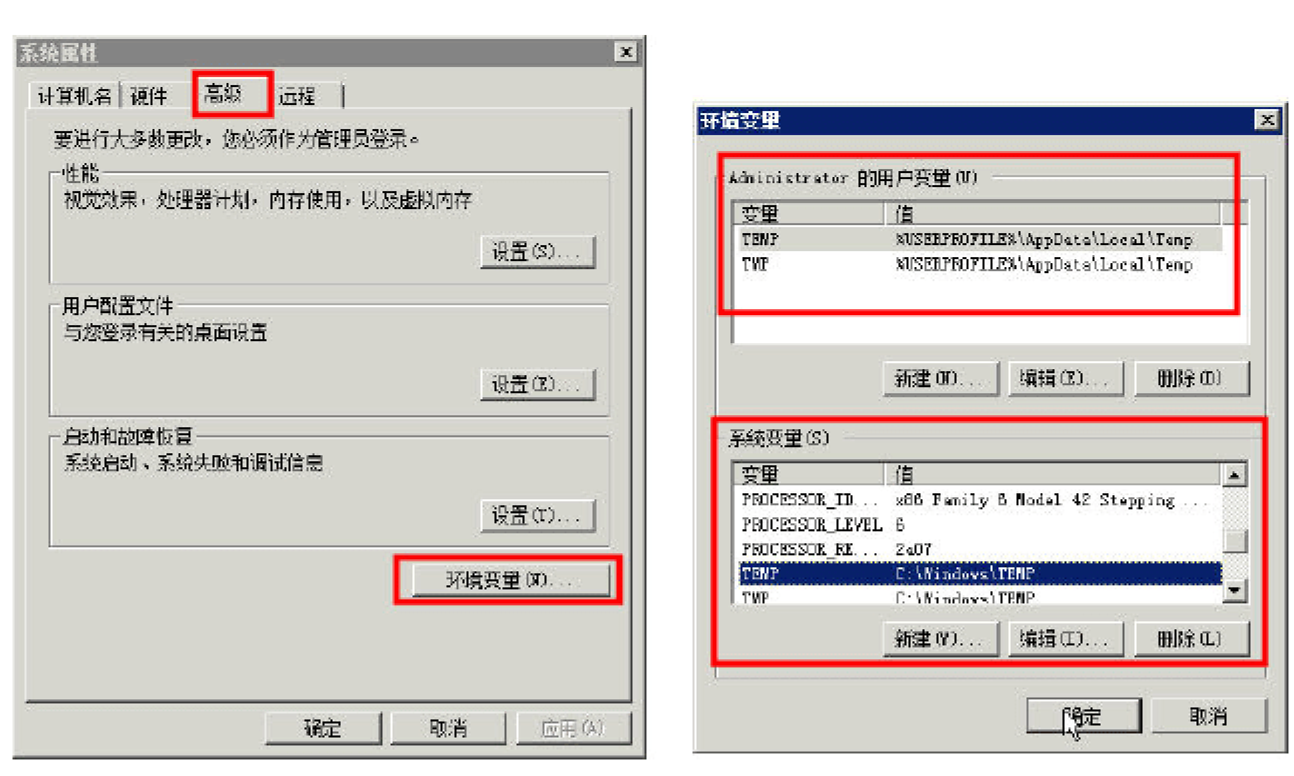


图 8-78　查看环境变量

用户也可以在命令提示符中输入 SET，查看当前用户的环境变量。一般情况下，常用的“Windows 环境变量”如下：

%AppDataDir%：当前用户的“应用程序数据”目录。

%BinaryComputerSid%：十六进制格式的计算机 SID。

%BinaryUserSid%：十六进制格式的当前用户 SID。

%CommonAppdataDir%：“所有用户”下的“应用程序数据”目录。

%CommonDesktopDir%：“所有用户”下的“桌面”目录。

%CommonFavoritesDir%：“所有用户”下的“Explorer 收藏夹”目录。

%CommonProgramsDir%：“所有用户”下的“程序”目录。

%CommonStartMenuDir%：“所有用户”下的“开始”菜单。

%CommonStartUpDir%：“所有用户”下的“启动”目录。

%ComputerName%：计算机的 NetBIOS 名称。

%CurrentProcessId%：主客户端进程的数字标识。

%CurrentThreadId%：主客户端线程的数字标识。

%DateTime%：当前时间（UTC）。

%DateTimeEx%：以毫秒为单位的当前时间（UTC）。

%DesktopDir%：当前用户的“桌面”目录。

%DomainName%：计算机的域名或工作组。

%FavoritesDir%：当前用户的“Explorer 收藏夹”目录。

%LastError%：配置期间遇到的上一个错误代码。

%LastErrorText%：上一个错误代码文本描述。

%LdapComputerSid%：LDAP 转义二进制格式的计算机 SID。

%LdapUserSid%：LDAP 转义二进制格式的当前用户 SID。

%LocalTime%：当前本地时间。

%LocalTimeEx%：以毫秒为单位的当前本地时间。

%LogonDomain%：当前用户所属的域。

%LogonServer%：验证当前用户身份的域控制器。

%LogonUser%：当前用户的用户名。

%LogonUserSid%：当前用户的 SID。

%MacAddress%：计算机上检测到的第一个 MAC 地址。

%NetPlacesDir%：当前用户的“网络邻居”目录。

%OsVersion%：操作系统为 Windows Server 2008、Windows Vista、Windows Server 2003、Windows XP 或未知。

%ProgramFilesDir%：Windows 程序文件目录。

%ProgramsDir%：当前用户的“程序”目录。

%RecentDocumentsDir%：当前用户的“最近的文档”目录。

%ResultCode%：客户端的退出代码。

%ResultText%：客户端的退出代码文本描述。

%ReversedComputerSid%：反向字节排序十六进制格式的计算机 SID。

%ReversedUserSid%：反向字节排序十六进制格式的当前用户 SID。

%SendToDir%：当前用户的“发送到”目录。

%StartMenuDir%：当前用户的“开始”菜单。

%StartUpDir%：当前用户的“启动”目录。

%SystemDir%：Windows 系统目录。

%SystemDrive%：运行操作系统的驱动器的名称。

%TempDir%：当前用户的“Temp”目录（由 Windows API 确定）。

%TimeStamp%：要执行的配置的时间戳。

%TraceFile%：跟踪文件的路径/名称。

%WindowsDir%：Windows 目录。

8.4.3　文件首选项

组策略包括文件首选项扩展。对于计算机或用户，使用此扩展可以：

- 将文件（或一个文件夹中的多个文件）复制到新位置，然后配置这些文件的属性。会根据需要创建新的子文件夹。
- 删除文件（或一个文件夹中的多个文件）并用源文件夹中的文件副本替换该文件。
- 修改文件（或一个文件夹中的多个文件）的属性。
- 删除文件（或一个文件夹中的多个文件）。
- 修改一个文件夹中具有特定扩展名的所有文件的属性，以及替换或删除这些文件。
- 修改特定文件夹中所有文件的属性，以及替换或删除这些文件。

创建文件首选项的步骤如下。

01 定位到“文件”首选项，在右侧空白窗格中右击，在弹出的快捷菜单中选择“新建→文件”选项，如图 8-79 所示。

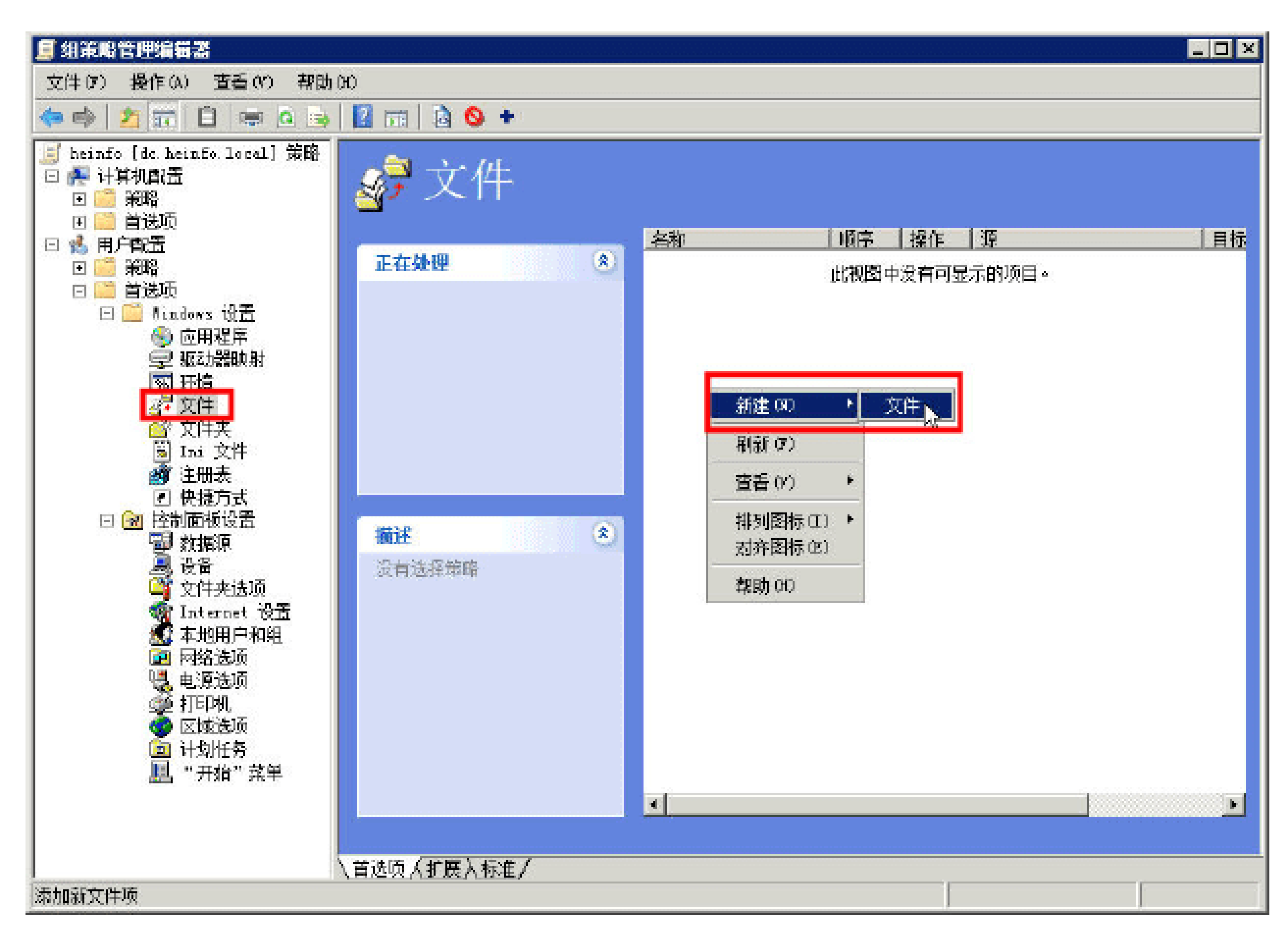


图 8-79　新建文件

02 打开“新文件 属性”对话框，在“操作”下拉列表中选择“创建”选项，在“源文件”文本框中选择图 8-69（8.4.1 节）中保存的一个文件，并以 UNC 的格式输入，在本例中为\\dc.heinfo.local\software\wrar400sc-x86-sc.exe，在“目标文件”中输入要保存到目标用户的路径，为本地路径，在此例中为 c:\temp\ wrar400sc-x86-sc.exe，如图 8-80 所示。然后在“公用”选项卡中选中“应用一次且不重新应用”复选框，如图 8-81 所示。

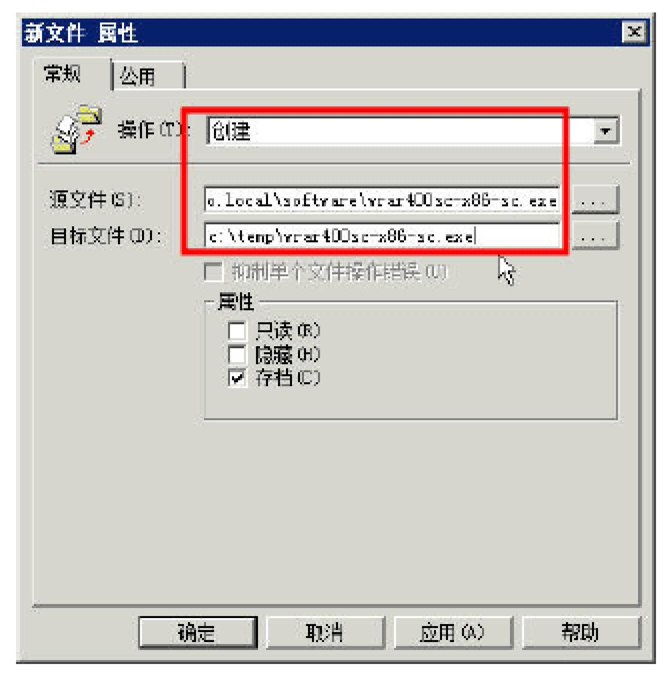


图 8-80　新文件

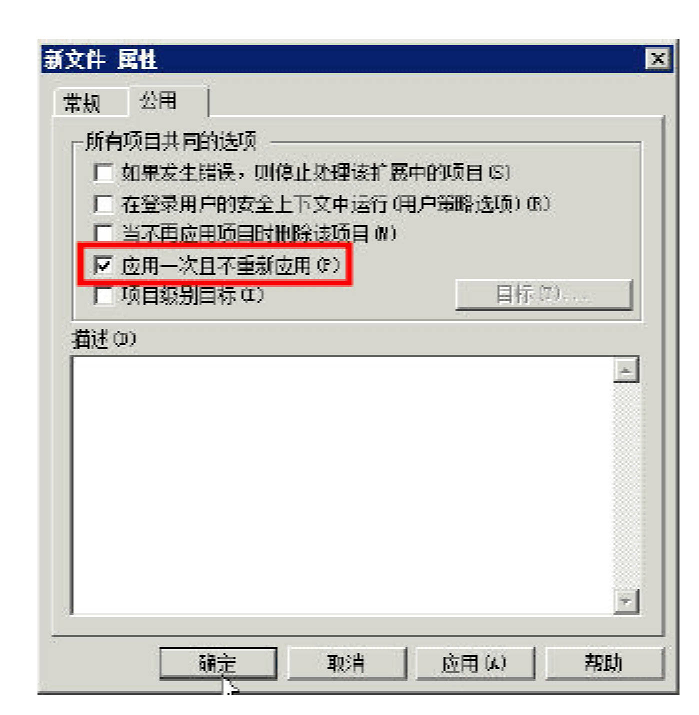


图 8-81　应用一次

8.4.4 Windows 设置中的文件夹首选项

Windows 设置中的文件夹首选项扩展可以实现如下功能：

- 创建文件夹并配置其属性。
- 修改文件夹并配置其属性。
- 删除文件夹及其内容。
- 仅当文件夹为空时删除文件夹。
- 删除文件夹（如临时文件文件夹）中的所有文件，而不删除该文件夹。
- 删除文件夹中的所有文件，而不删除子文件夹。

在 Windows 设置中，创建文件夹首选项的步骤如下。

01 定位到“Windows 设置→文件夹”首选项，在右侧空白窗格中右击，在弹出的快捷菜单中选择“新建→文件夹”选项，如图 8-82 所示。

02 在“新文件夹 属性”对话框中，在“操作”下拉列表中选择“更新”选项，在“路径”文本框中输入 c:\temp，如图 8-83 所示，其他保持默认值。

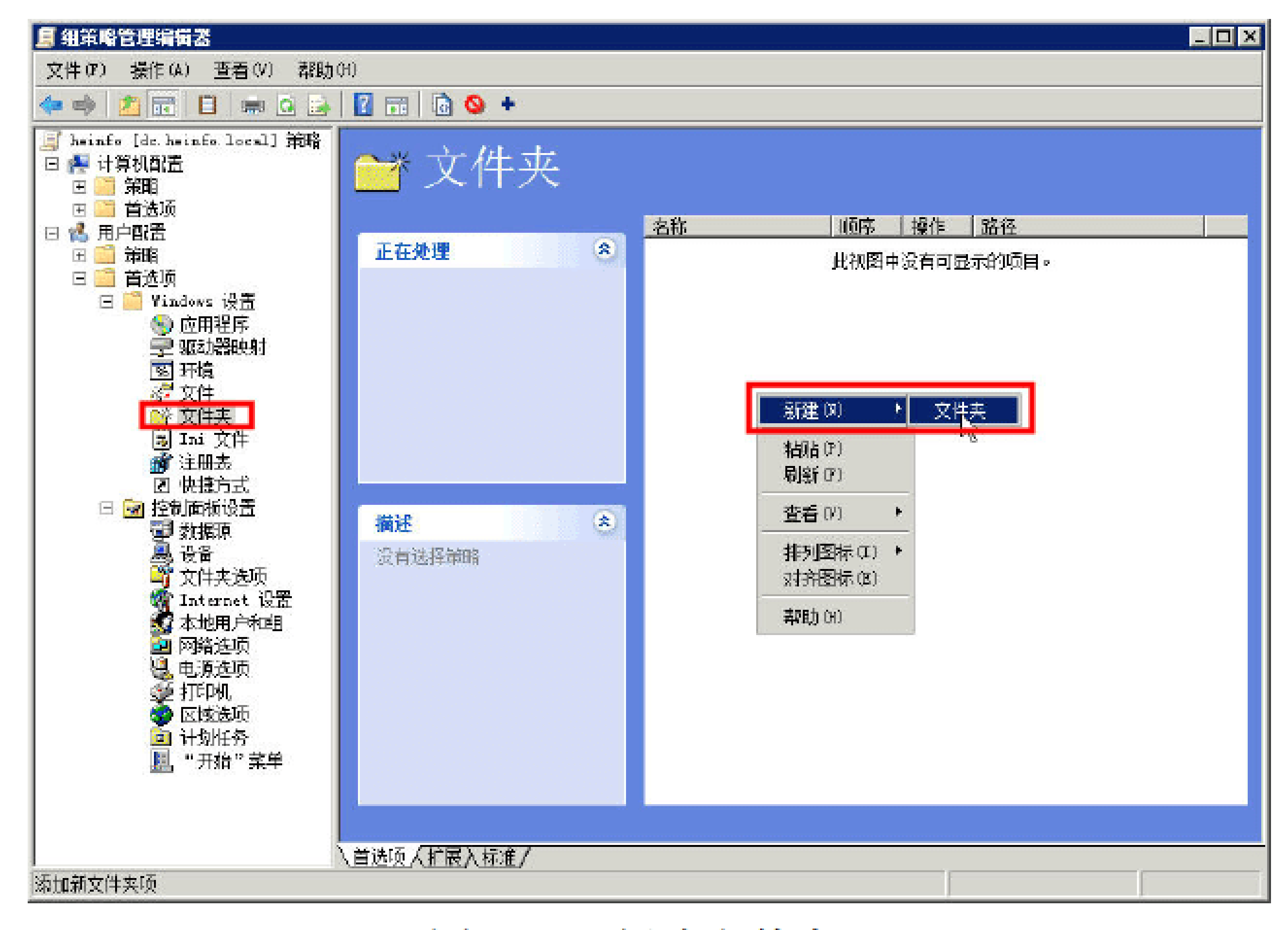


图 8-82 新建文件夹

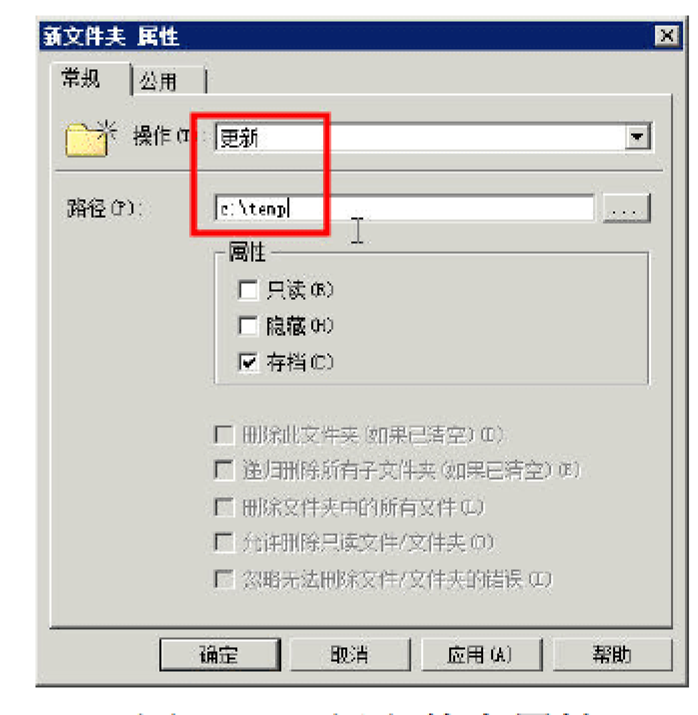


图 8-83 新文件夹属性

03 设置完成之后，单击“确定”按钮。

04 经过上述设置，将会在目标计算机上的 C 盘创建 TEMP 文件夹。

8.4.5 控制面板中的文件夹首选项

控制面板中的文件夹首选项允许用户为 Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP 配置各种 Windows Explorer 设置（如文件类型和应用程序启动关联）和文件夹视图选项。

在控制面板中，创建文件夹首选项的步骤如下。

01 定位到“控制面板设置→文件夹选项”首选项，在右侧空白窗格中右击，在弹出的快捷

菜单中选择“新建→文件夹选项（Windows Vista）”选项，如图 8-84 所示。



说 明

文件夹选项包括 Windows XP（用于 Windows XP、Windows Server 2003）、Windows Vista（用于 Windows Vista、Windows Server 2008）文件夹首选项，在本例中以 Windows Vista 为例，Windows XP 的操作与此类似。

02 在“新文件夹选项（Windows Vista）属性”对话框中，设置文件夹选项，如图 8-85 所示。

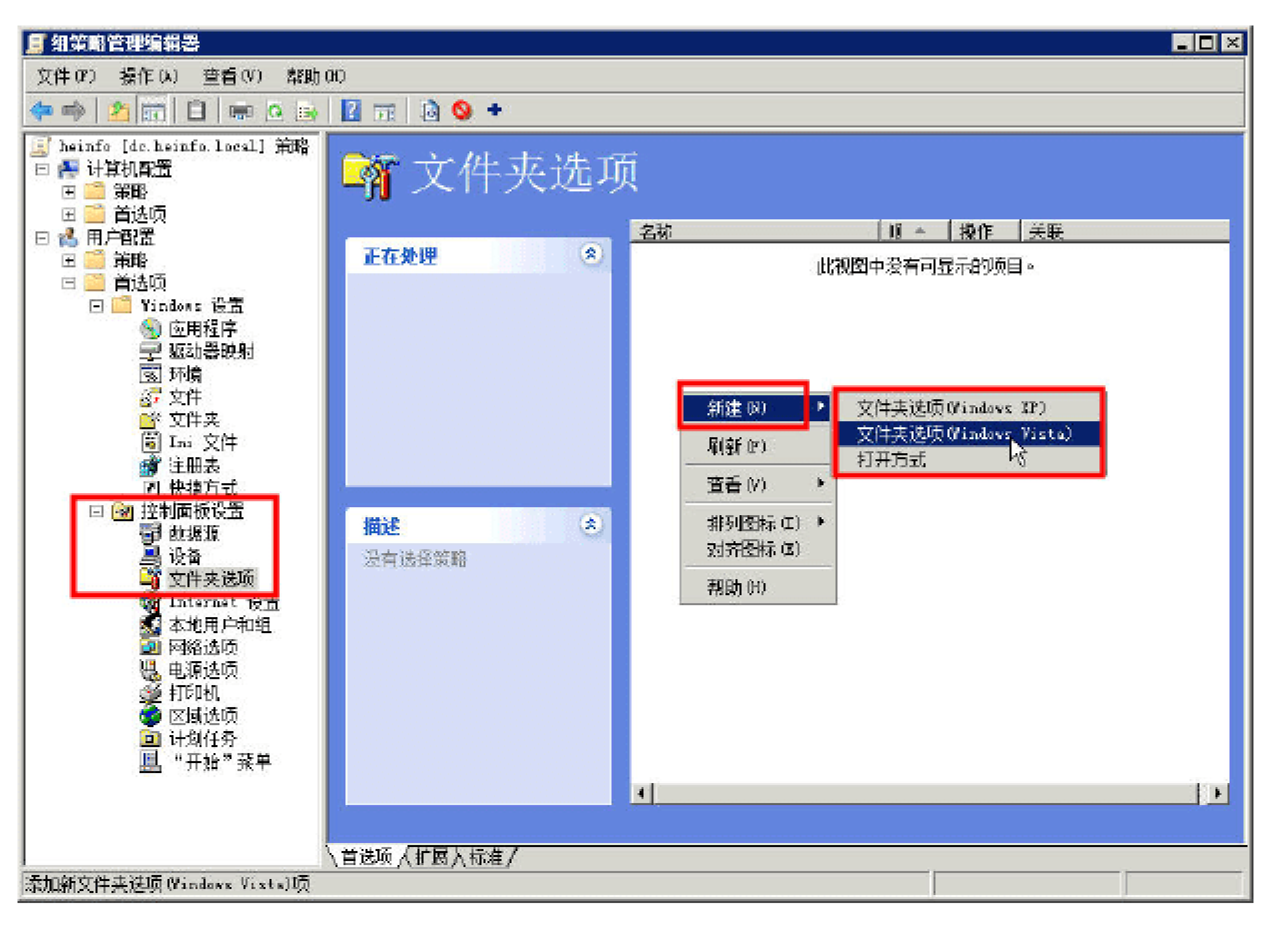


图 8-84　新建文件夹选项

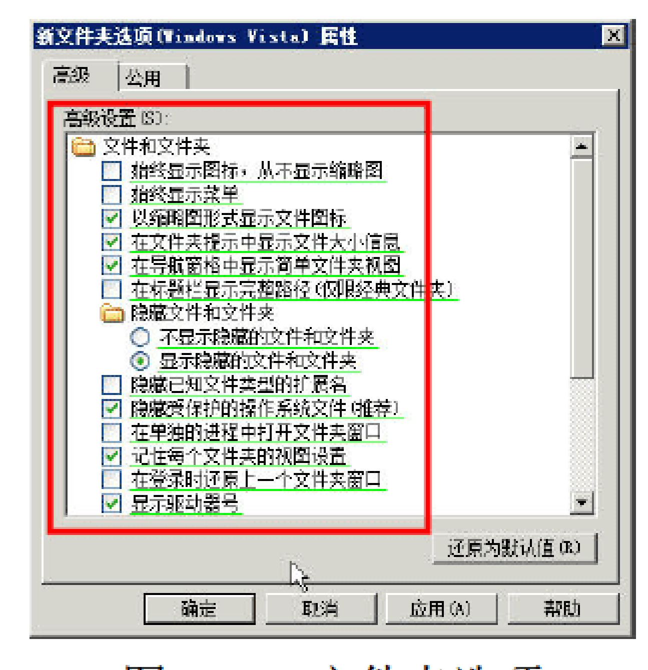


图 8-85　文件夹选项

8.4.6 Internet 设置首选项

组策略包括 Internet 设置首选项扩展。对于用户，使用该扩展可以：

- 对 Internet 设置进行特定配置。
- 对 Internet 设置进行初始配置，但允许最终用户进行更改。
- 配置几个 Internet 设置，而其他设置由每个最终用户进行配置（例如，可以指定代理服务器设置，从而允许用户修改辅助功能选项）。

设置 Internet 首选项的步骤如下。

01 定位到“控制面板设置→Internet 设置”，在右侧空白窗格中右击，在弹出的快捷菜单中选择“新建→Internet Explorer 7”选项，如图 8-86 所示。



说 明

可以创建用于 IE5、IE6 的 Internet Explorer 5 和 6 设置，以及用于 IE7 的 Internet Explorer 7，可根据需要选择。

02 在弹出的“新 Internet Explorer 7 属性”对话框中，可以进行 IE7 的每项设置，如图 8-87 所示。

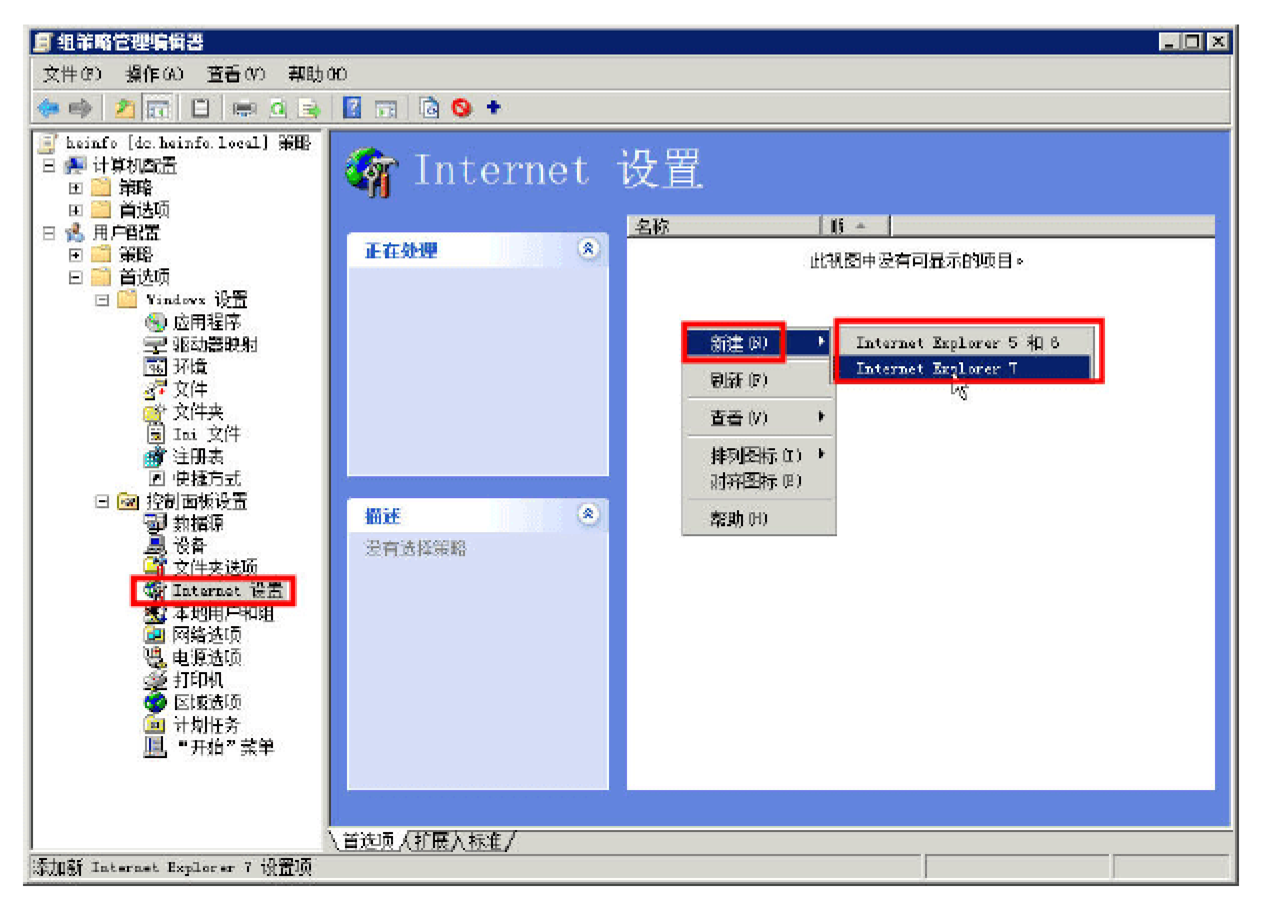


图 8-86　新建 IE7 设置

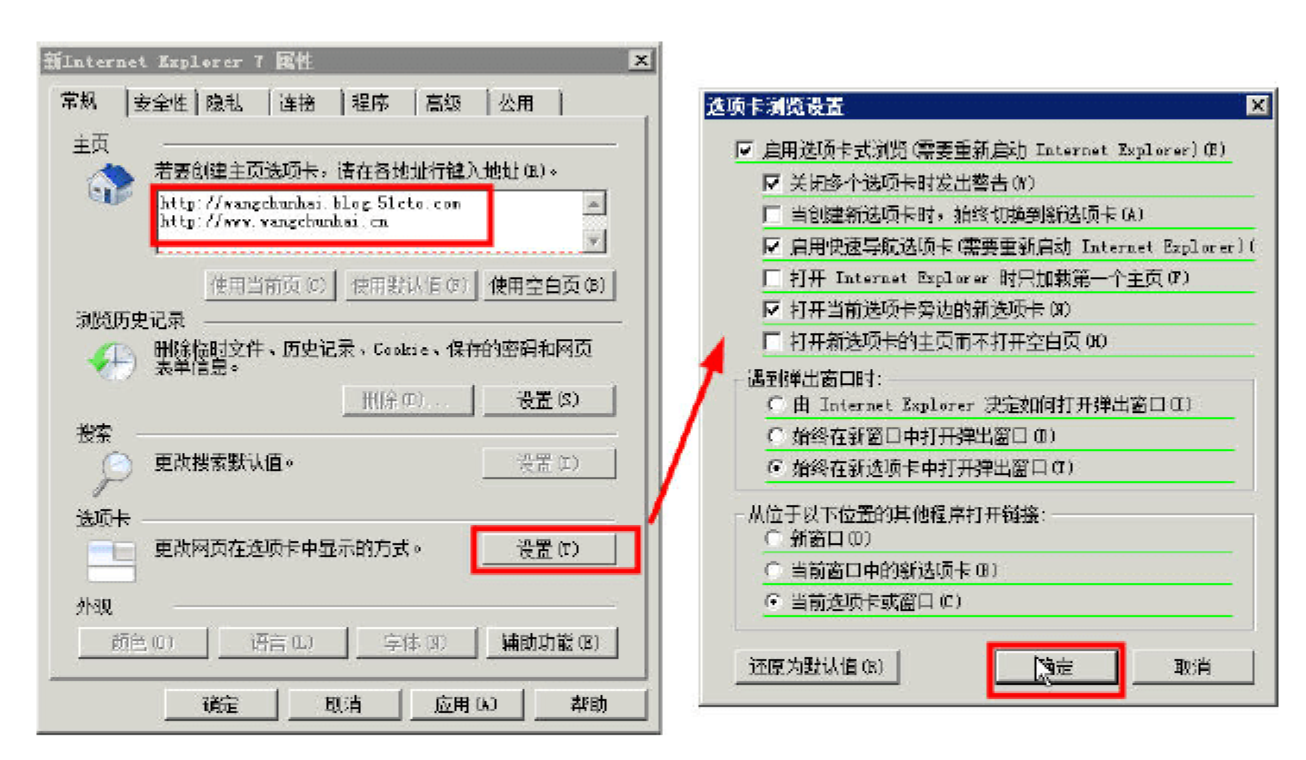


图 8-87　Internet Explorer 设置

用户可根据需要，对每个选项卡、每个选项做出设置。

8.4.7　本地用户和组首选项

组策略包括本地用户和组首选项扩展。该扩展允许用户集中管理域成员计算机上的本地用户和组，在本小节中，以创建名为 test001 用户的实例，介绍这个策略应用。主要步骤如下。

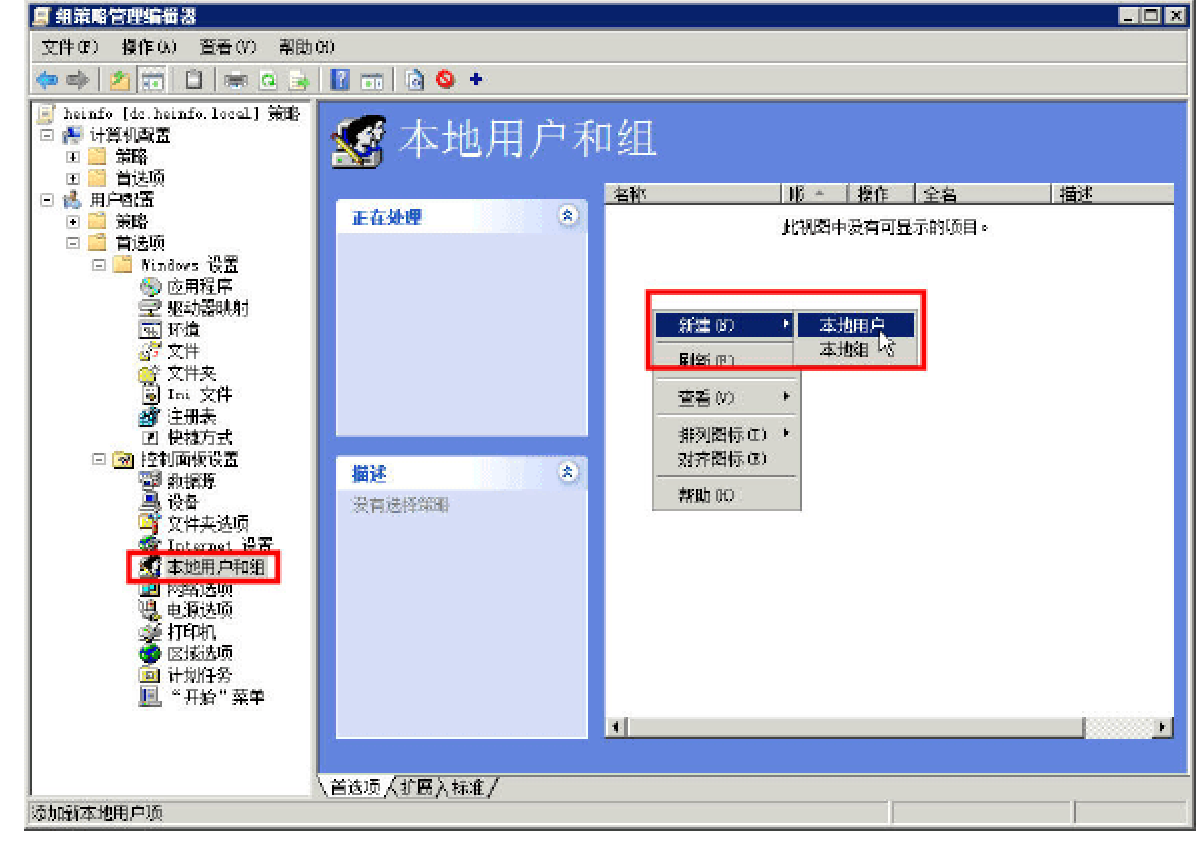


图 8-88　新建用户

01 定位到“控制面板设置→本地用户和组”，在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→本地用户”选项，如图 8-88 所示。

02 在“新本地用户 属性”对话框中，在“操作”下拉列表中选择“创建”选项，在“用户名”文本框处输入 test001，设置密码为 a1b2c3D4，如图 8-89 所示。在

“公用”选项卡中选中“应用一次且不重新应用”复选框，如图 8-90 所示。

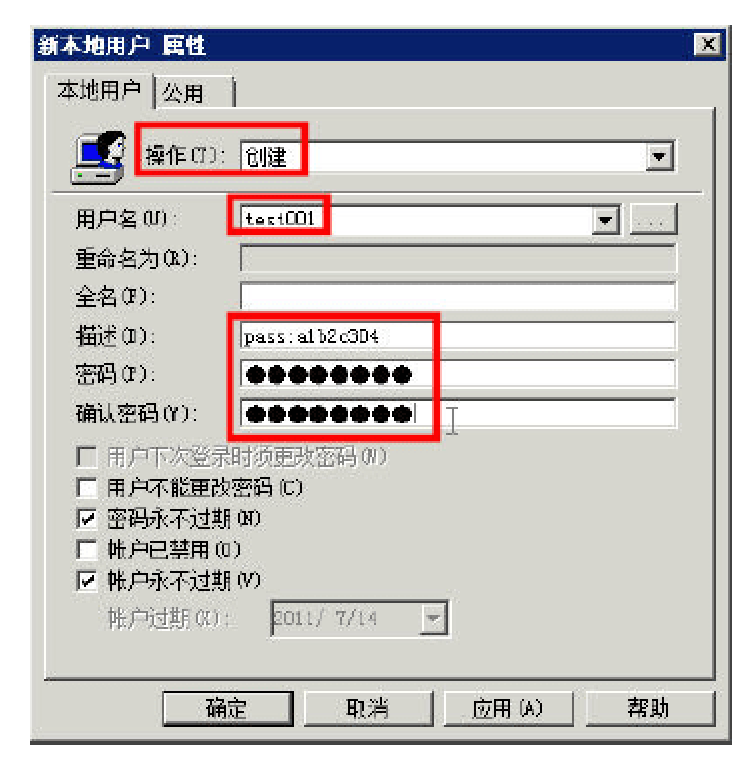


图 8-89　设置新建用户信息

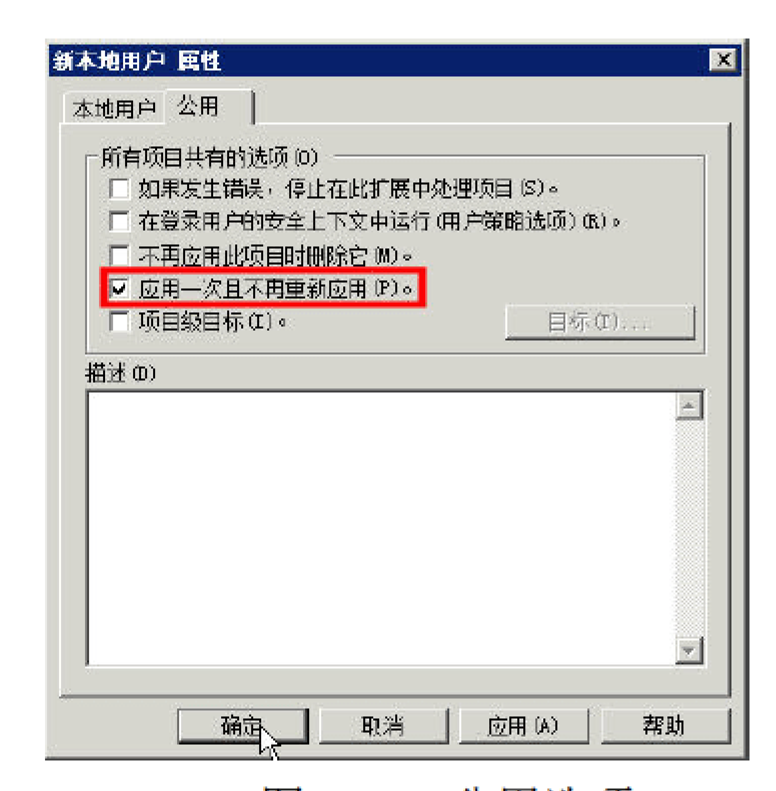


图 8-90　公用选项

8.4.8　网络选项首选项

组策略包括网络选项首选扩展。通过此扩展可以配置虚拟专用网络（VPN）或拨号网络连接。下面以创建 VPN 连接为例介绍这个选项的使用，步骤如下。

01 定位到“控制面板设置→网络选项”选项，在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→VPN 连接”选项，如图 8-91 所示。

02 在“新 VPN 属性”对话框，在“操作”下拉列表中选择“创建”选项，在“连接名称”文本框处输入新建 VPN 连接的名称，例如 vpn-test，在“IP 地址”文本框处输入 VPN 服务器的地址，例如 1.2.3.4（在实际的环境中，须用要拨号的 VPN 服务器的 IP 地址代替），如图 8-92 所示。在“公用”选项卡选择“应用一次且不重新应用”，其他保持默认值。

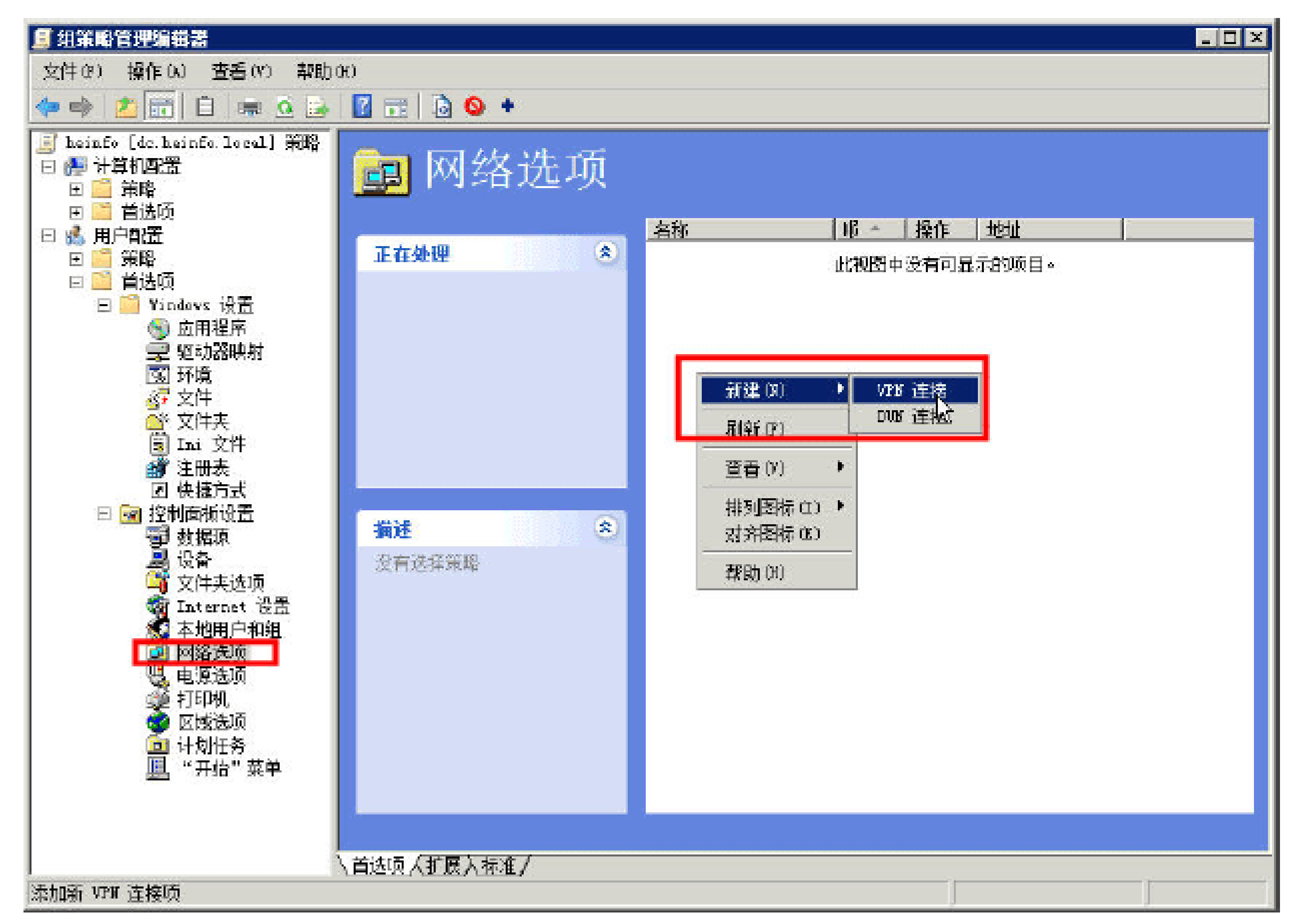


图 8-91　新建 VPN 连接

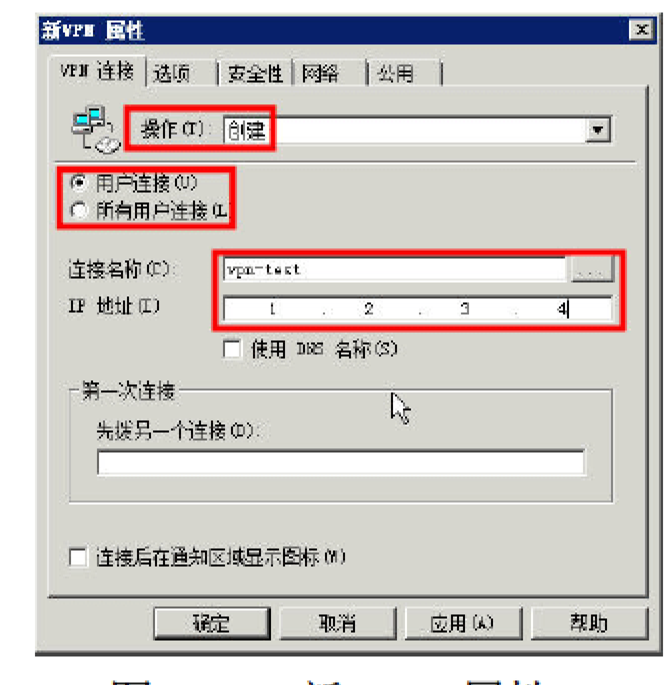


图 8-92　新 VPN 属性

8.4.9　电源首选项

组策略包括电源选项首选项扩展。该扩展允许用户配置 Windows Server 2003 和 Windows XP

电源选项，创建电源选项的步骤如下。

01 定位到“控制面板设置→电源选项”，在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→电源选项（Windows XP）”，如图 8-93 所示。

02 在“新电源选项（Windows XP）属性”对话框中，根据需要，设置电源选项，如图 8-94 所示。

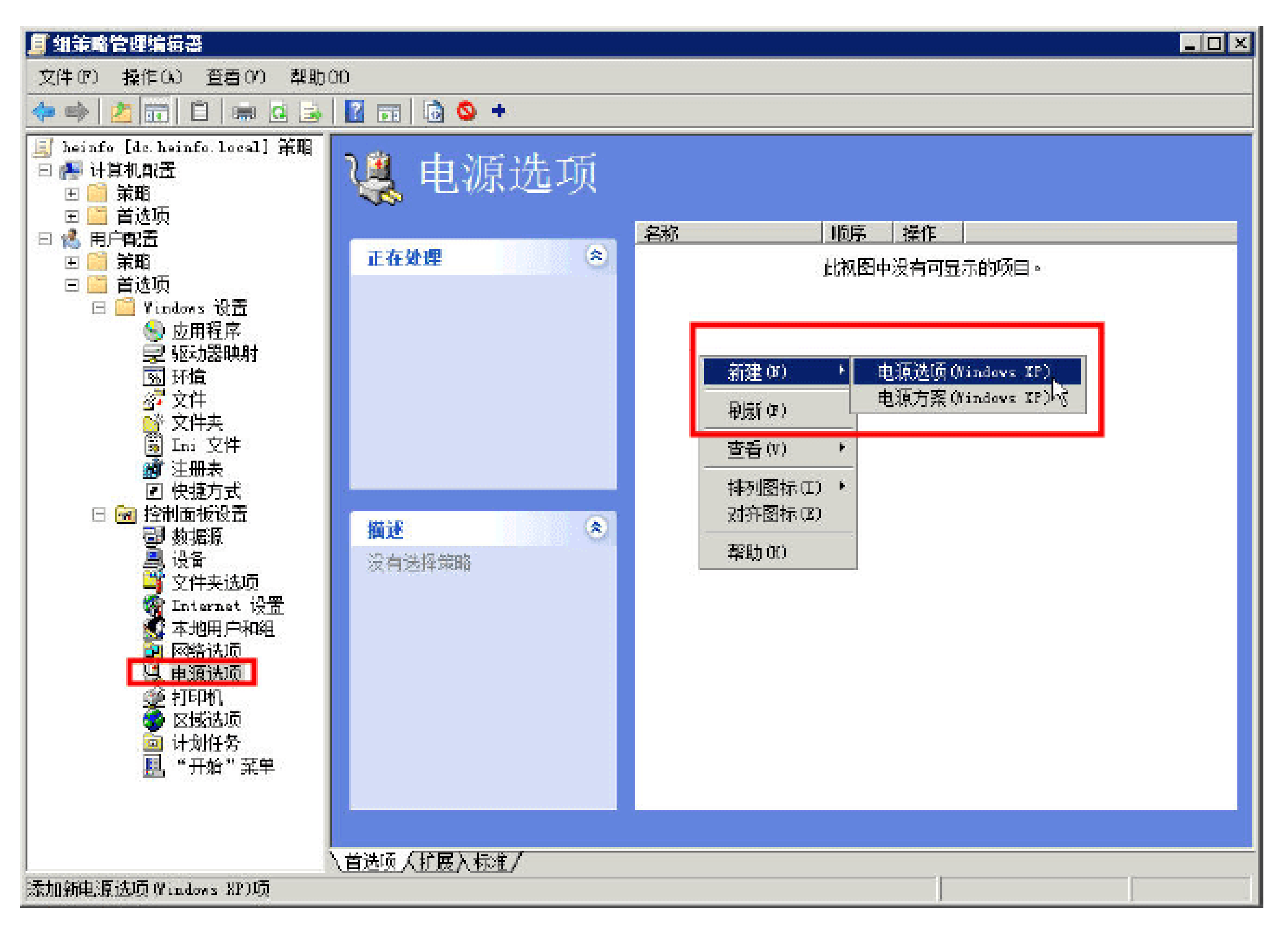



图 8-93　创建电源选项

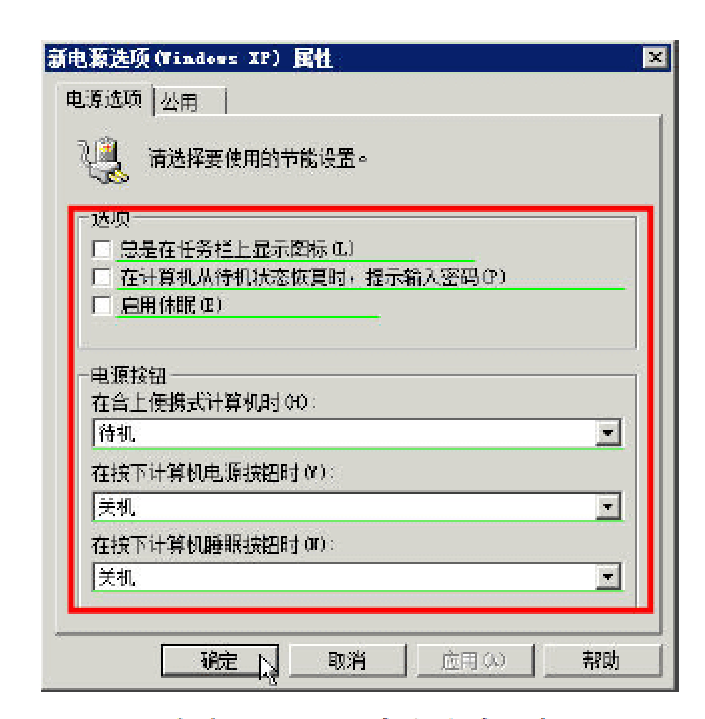


图 8-94　电源选项

8.4.10　开始菜单首选项

组策略包括开始菜单首选扩展。对于用户来说，使用该扩展可以：

- 对“开始”菜单进行特定配置。
- 对“开始”菜单进行初始配置，但允许最终用户进行更改。
- 配置几个“开始”菜单设置，而将其他设置留给每个最终用户去配置。

下面介绍开始菜单首选项的配置方法，步骤如下：

01 定位到“控制面板设置→开始菜单”，在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→开始菜单（Windows Vista）”选项，如图 8-95 所示。

说 明

开始菜单包括用于 Windows Server 2003 与 Windows XP 的“开始菜单（Windows XP）”与用于 Windows Server 2008 与 Windows Vista 的“开始菜单（Windows Vista）”两种，可根据需要选择。

02 在弹出的对话框中，根据需要设置“常规”与“经典”开始菜单项目，如图 8-96、图 8-97 所示。

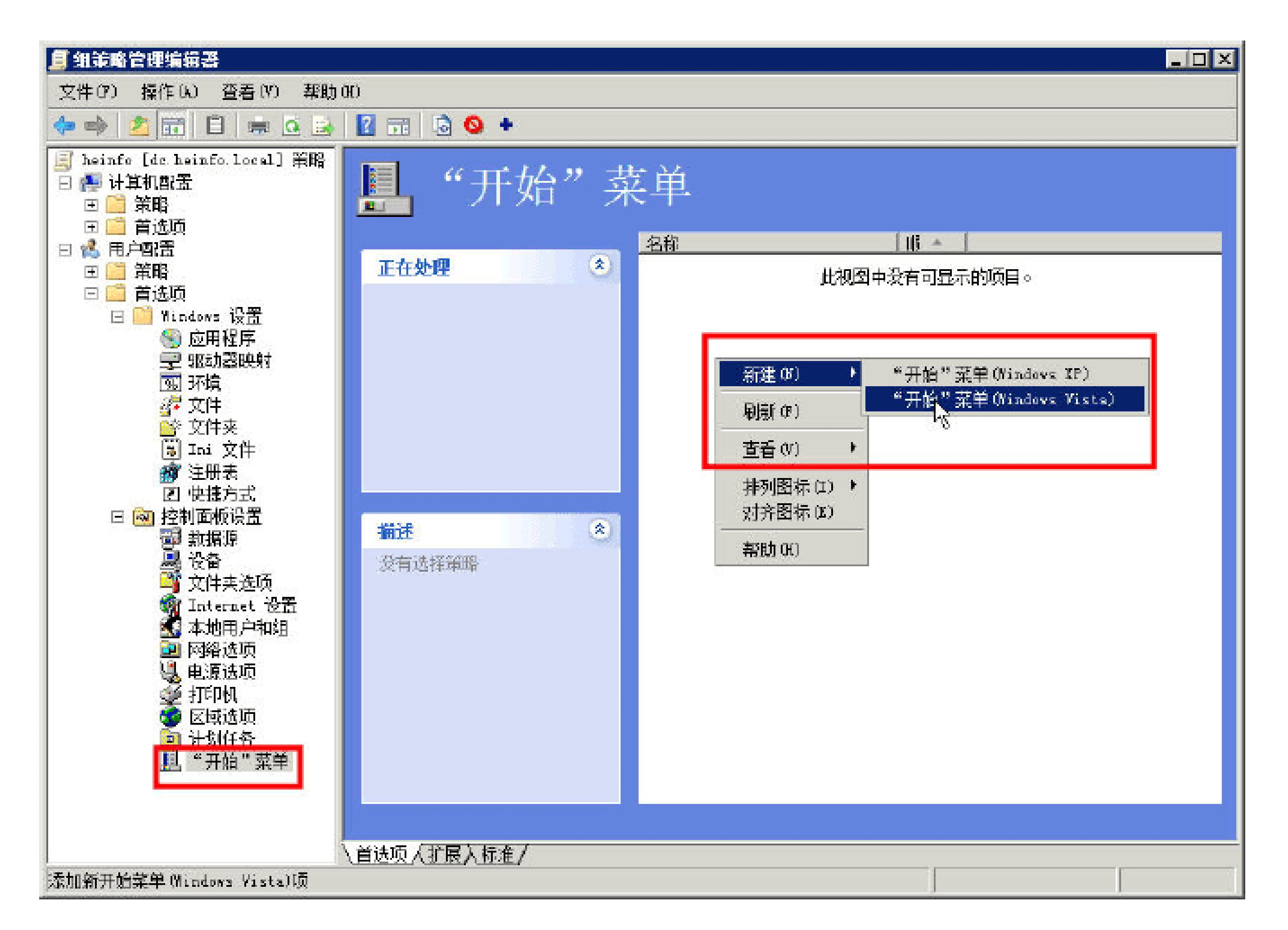


图 8-95　新建开始菜单

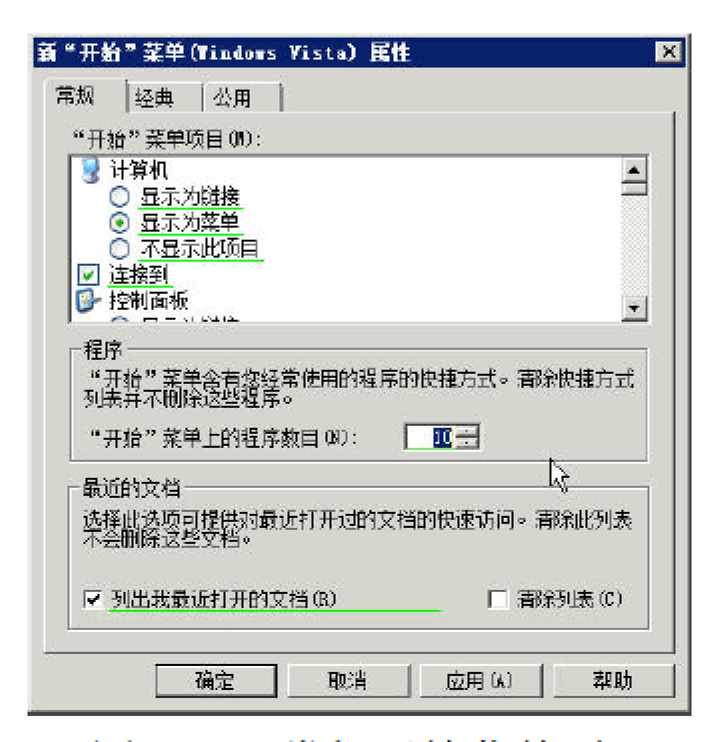


图 8-96　常规开始菜单项目

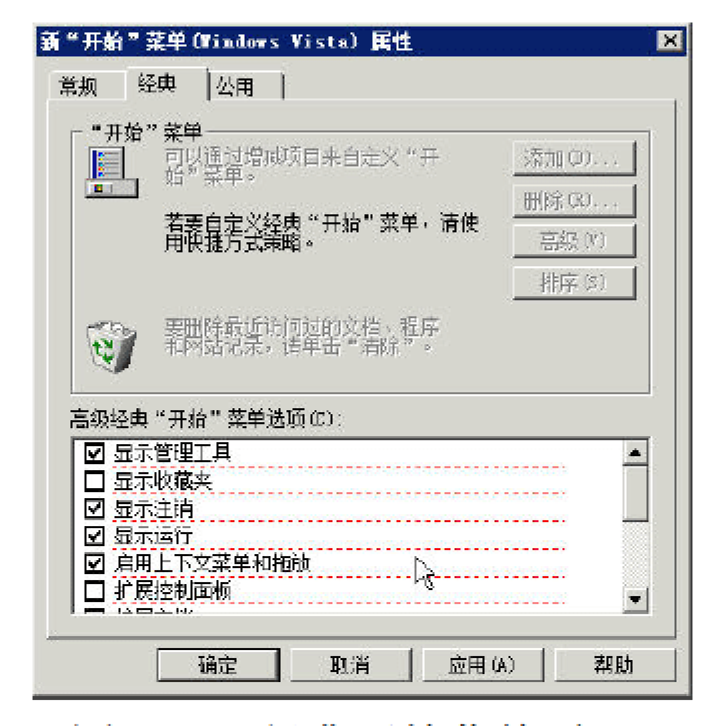


图 8-97　经典开始菜单项目

03　如果要为 Windows XP 操作系统定制开始菜单，可参照步骤 1～2 的操作，在图 8-95 中选择“新建→开始菜单（Windows XP）”选项，创建用于 Windows XP 的开始菜单，这些不再赘述。

8.5　使用组策略分发软件

向网络中的多台计算机安装相同的软件，是一项非常麻烦的工作，需要在各台计算机上重复运行安装过程。不过，利用组策略可以同时为多台计算机部署安装应用程序，管理员无须到每一台计算机上去安装，既方便又快捷。

8.5.1　发布软件前的准备工作

对于不同的软件，要用不同的方法进行部署。用户常用的软件类型有以下几种：

（1）Microsoft 的 MSI 安装程序包：主要包括 Microsoft 的 MSI 安装程序包及所有的 Microsoft Office 类软件，如 Word、Excel、PowerPoint 等，还包括其他一些带有 MSI 安装包的软件。这些软件允许“管理员安装”。

（2）其他 MSI 安装程序包：如 NOD32 杀毒软件的安装程序，这些软件没有“管理员安装”选项。

（3）普通的 EXE 安装程序（即扩展名为.exe 的安装程序），如 Microsoft 开发工具 VC、VB 等；以及一些常用软件，如 ACD See、Adobe Reader、WinRAR、Fox mail 等。这些软件允许重新打包和定制。

（4）一些加密或专业的软件，如金山毒霸、KV2011 等杀毒软件，这些软件不允许重新打包，或者打包后在不同的计算机上不能使用。重新打包的软件，要在不同的计算机、不同的操作系统（至少要能同时兼容 Windows 2000 与 Windows XP、Windows 7）上使用。

对于（1）种软件，可以使用其自身提供的工具（或安装参数）进行“管理员安装”后供用户使用。对于（2）、（3）种软件，可以使用“Install Rite”软件重新打包这些安装程序。而对于（4）种不能打包的软件，只能由用户手动选择或者使用 Auto IT 来制作安装脚本进行安装。

发布软件前的具体准备工作如下：

（1）首先，需要为组策略发布软件创建一个保存软件安装包（或安装程序）的文件夹，并将此路径设置为共享。

（2）然后，根据软件的不同，在“安装程序文件夹”中创建不同的文件夹。例如，创建 input 的文件夹，用来保存输入法的安装程序。

Windows 主要有两种安装程序包，一种是扩展名为.EXE 的安装程序，另一种是扩展名为.MSI 的安装程序。不过，使用组策略发布软件时，只支持扩展名为.MSI 的安装程序，对于扩展名为.EXE 的传统安装程序则需要创建与其对应的扩展名为.ZAP 的文本文件。

ZAP 文件的格式为：

[Application]　　文件头，是必须有的。

FriendlyName=　　后面输入安装程序的名称，并以英文双引号（“”）包含。

SetupCommand=　　后面输入安装程序的名称，可以输入相对路径如 setup.exe，也可以输入绝对路径（必须是 URL 格式），例如：\\安装程序文件夹\input\znwb5807.exe。如果安装程序不带参数，必须用两个英文的双引号包含。

说 明

在 Windows 2000 中，用一个双引号包含即可，但在 Windows Server 2003/2008 中，必须用两个双引号。如果安装程序带有参数，可以用一个双引号包含，如安装程序的执行过程是 setup.exe /g，则可以输入 Setup Command=“serup.exe”/g。这一设置对于 Windows Server 2003/2008 同样适用。“Display Version=”后面输入安装程序的版本号，“Publisher=”后面输入开发软件的所属公司名称。创建好 ZAP 文件，就可以直接发布 EXE 文件了。

一个创建好的 ZAP 文件内容如下所示：

```
[Application]
FriendlyName="WinRAR 压缩解压缩软件 32 位版本"
SetupCommand=""wrar400sc-x86-sc.exe""
DisplayVersion=4.0
Publisher=软众信息 WinRAR 中国区
```

8.5.2　使用组策略发布 EXE 软件

下面通过一个具体的实例，介绍创建、编写 ZAP 文件方法，以及如何使用组策略发布 EXE 软件，步骤如下。

01 打开“资源管理器”，进入“文件夹选项”，在“查看”选项卡中，选中“显示隐藏的文件和文件夹”单选按钮，取消选中“隐藏已知文件类型的扩展名”复选框，如图 8-98 所示。

02 在 E 盘 software 文件夹中，复制 winrar 压缩软件，文件名为 wrar400sc-x86-sc.exe，创建一个文本文件，设置文件名为 winrarx-400-x86.zap，并用“记事本”打开该文件，填写各项，如图 8-99 所示。

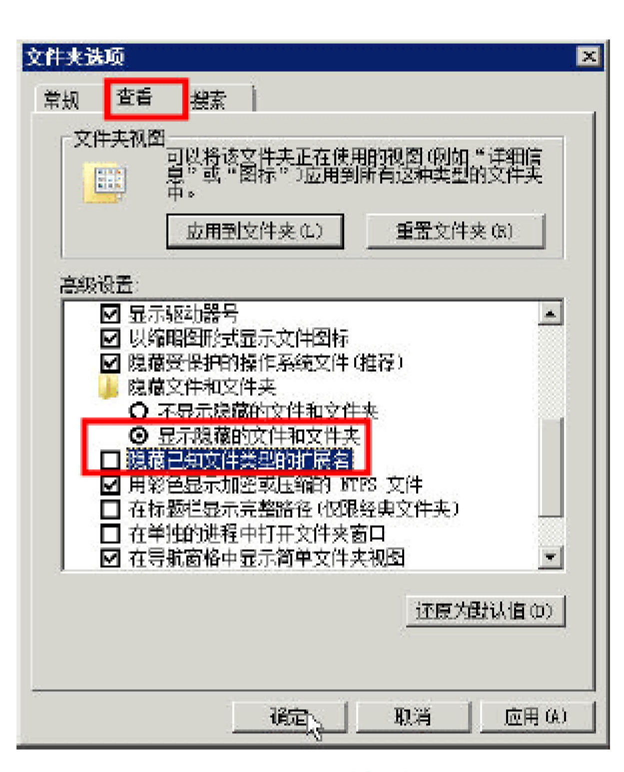



图 8-98　文件夹选项

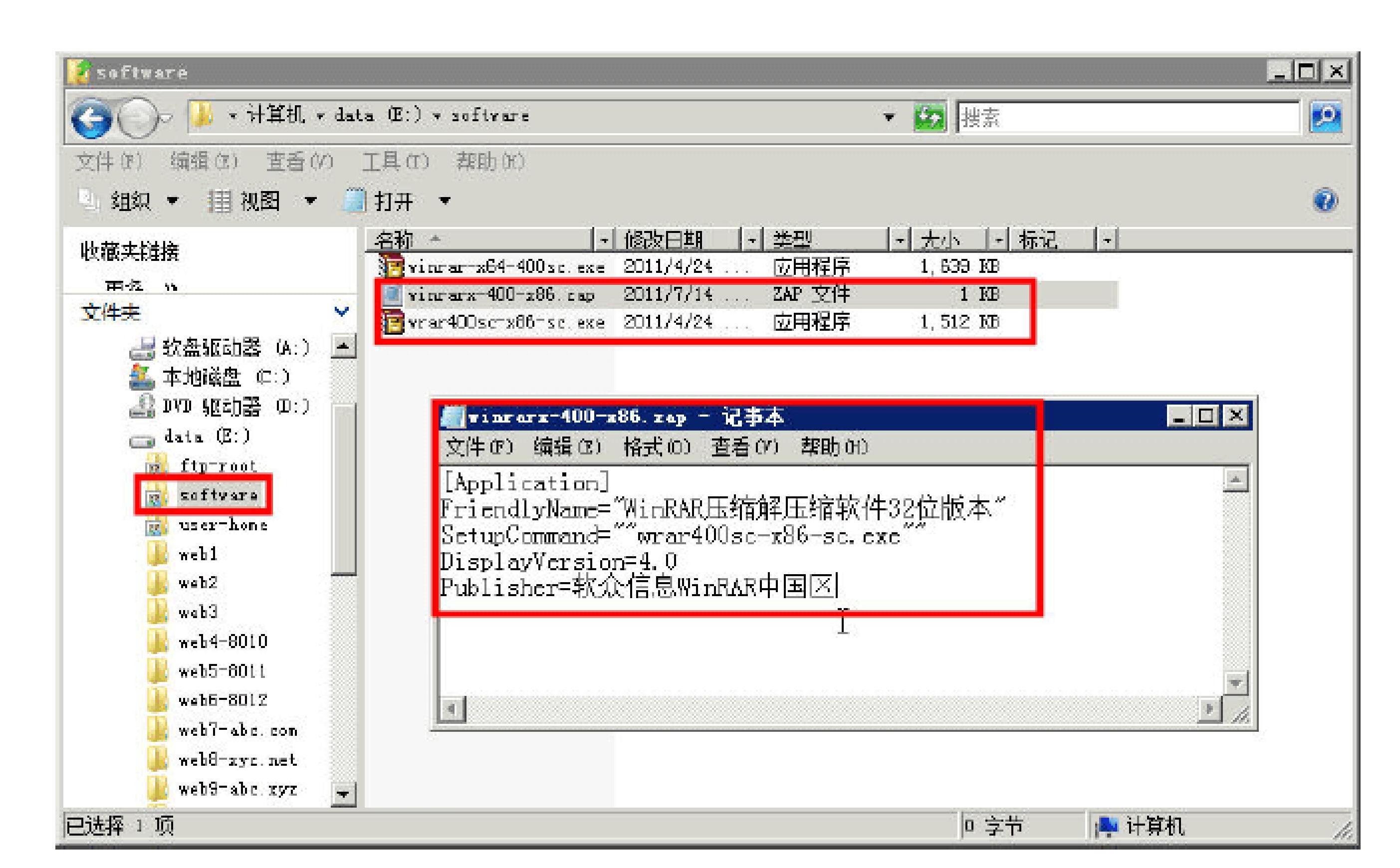


图 8-99　编写 ZAP 文件

03 打开“信息技术学院”组织单位的“组策略管理编辑器”，定位到“用户配置→策略→软件设置”，用鼠标右击“软件安装”，在弹出的快捷菜单中选择“属性”选项，如图 8-100 所示。

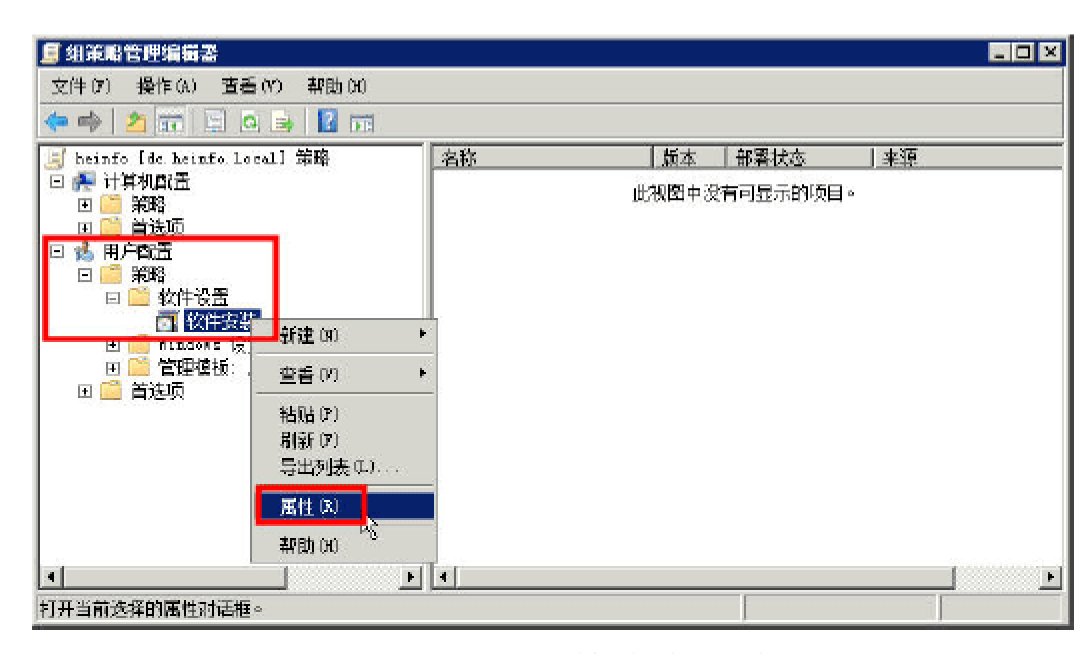


图 8-100　软件安装属性

04 在“软件安装 属性”对话框的“常规”选项卡中，在“默认程序数据包位置”文本框中输入保存软件分发路径的共享位置，在本例中为\\DC.heinfo.local\software，如图 8-101 所示。

05 在“类别”选项卡，单击“添加”按钮，添加软件包的分类，例如，在本例中，添加了 Office、常用软件、杀毒软件等软件类别，如图 8-102 所示。

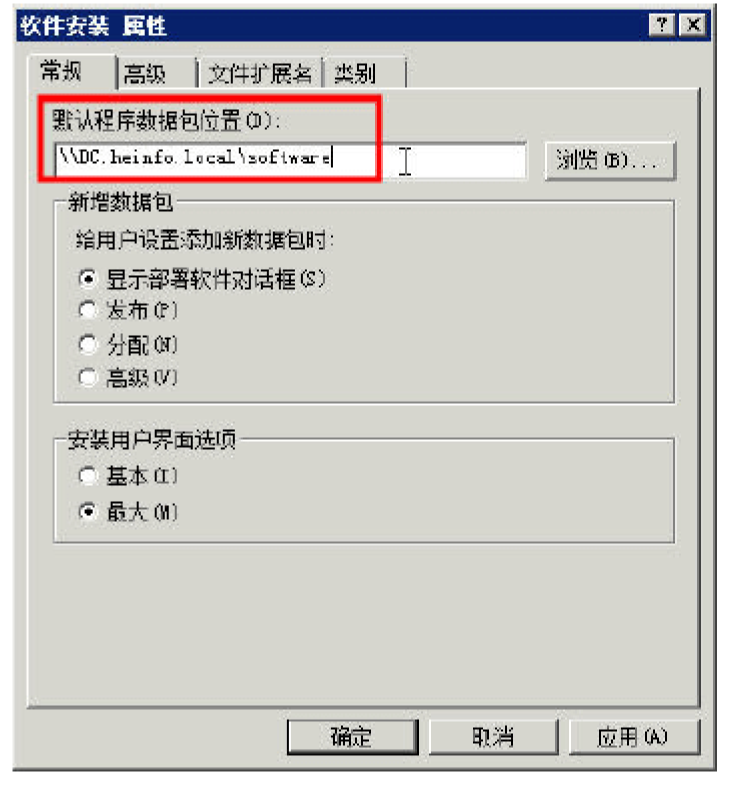


图 8-101　指定默认程序数据包位置

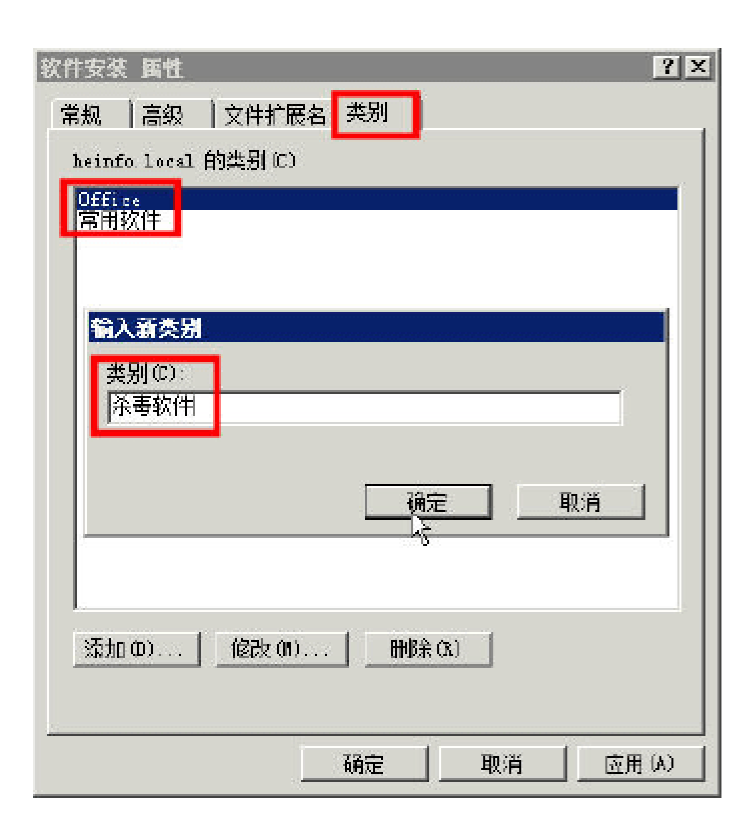


图 8-102　软件类别

06 返回到“组策略管理编辑器”中，在右侧的空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→数据包”选项，如图 8-103 所示。

07 在“打开”对话框中，会自动打开图 8-101 中指定的路径，在下拉列表中选择“ZAW 早期版本应用程序数据(*.zap)”选项，然后选择前面创建的“winrarx-400-x86.zap”文件，如图 8-104 所示。

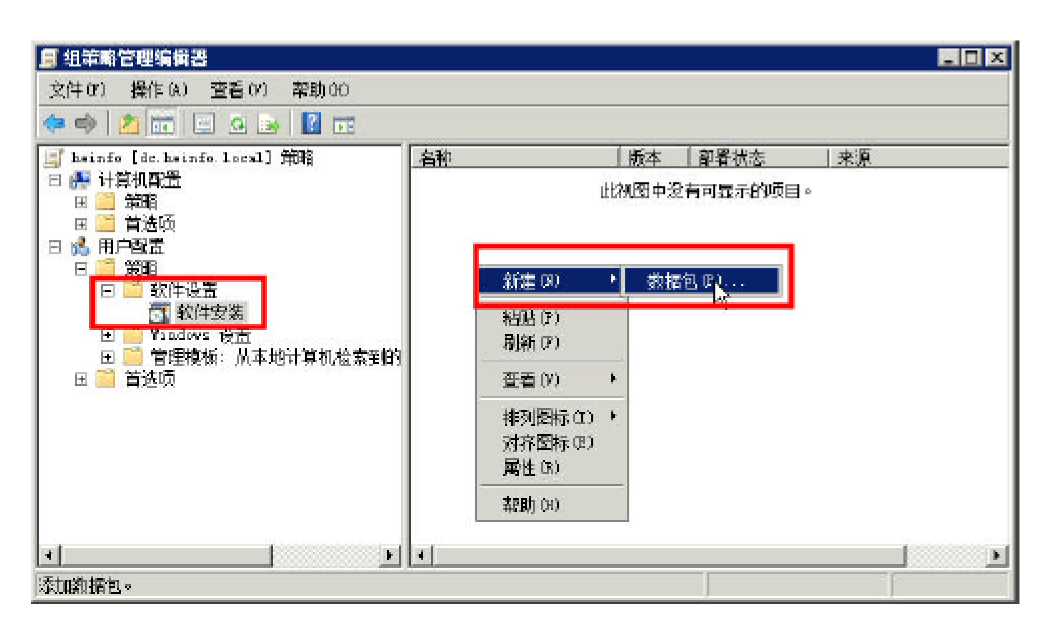


图 8-103　新建数据包

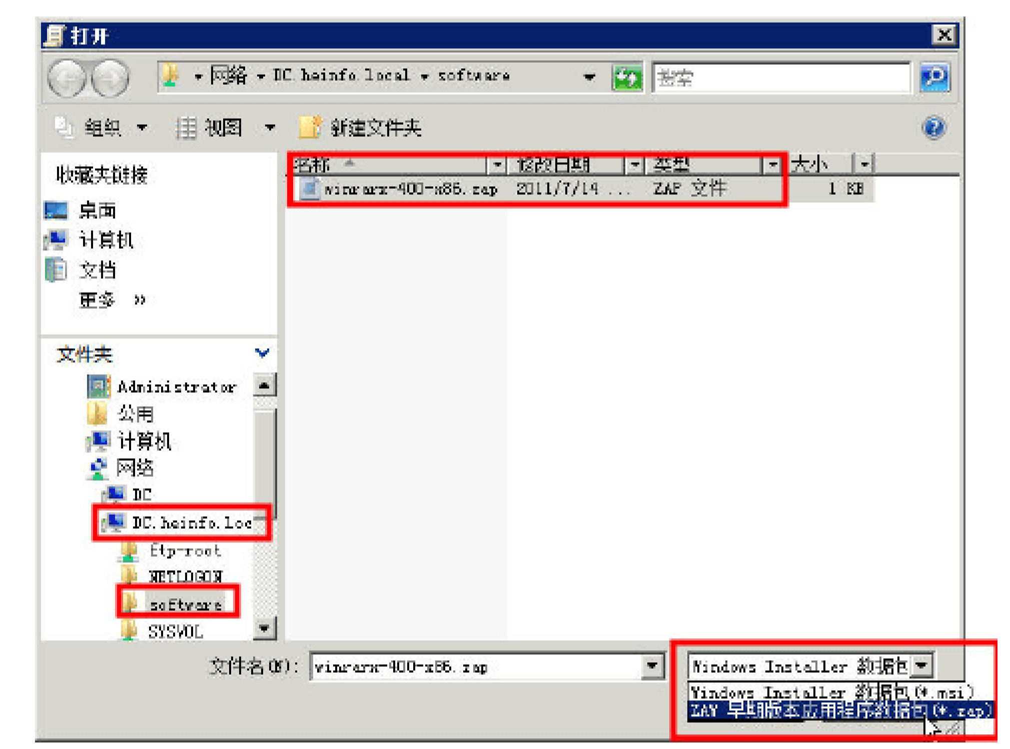
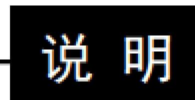


图 8-104　选择 ZAP 包



说 明

如果要发布的软件保存在其他位置，请在“文件名”文本框中，输入 UNC 路径，或者在“网络”位置浏览选择。

08 在“部署软件”对话框中，选择“已发布”选项，如图 8-105 所示。

09 创建要发布的软件包后，显示如图 8-106 所示。

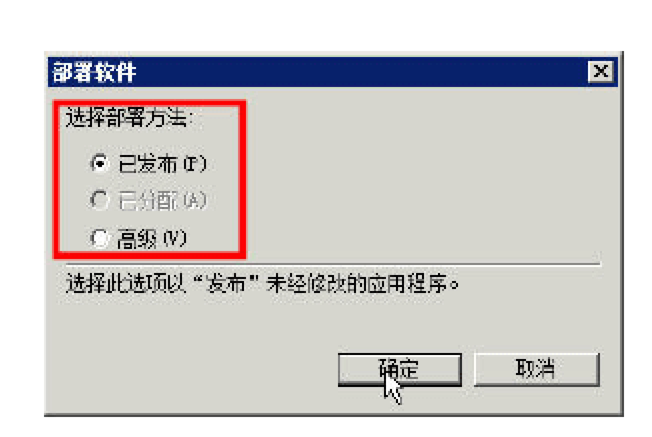


图 8-105　已发布

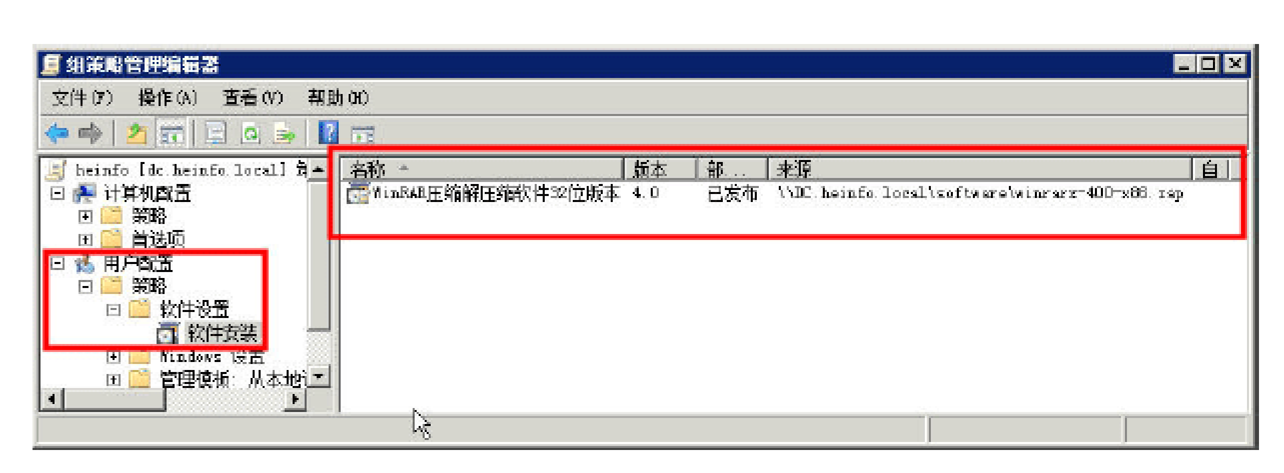


图 8-106　发布的软件包

10 用鼠标双击发布的软件，弹出软件包属性对话框，在“常规”选项卡中，可以修改软件包的名称（如图 8-107 所示），在“类别”选项卡中，选择发布的软件包的类型，在此选择“常用软件”选项，如图 8-108 所示。

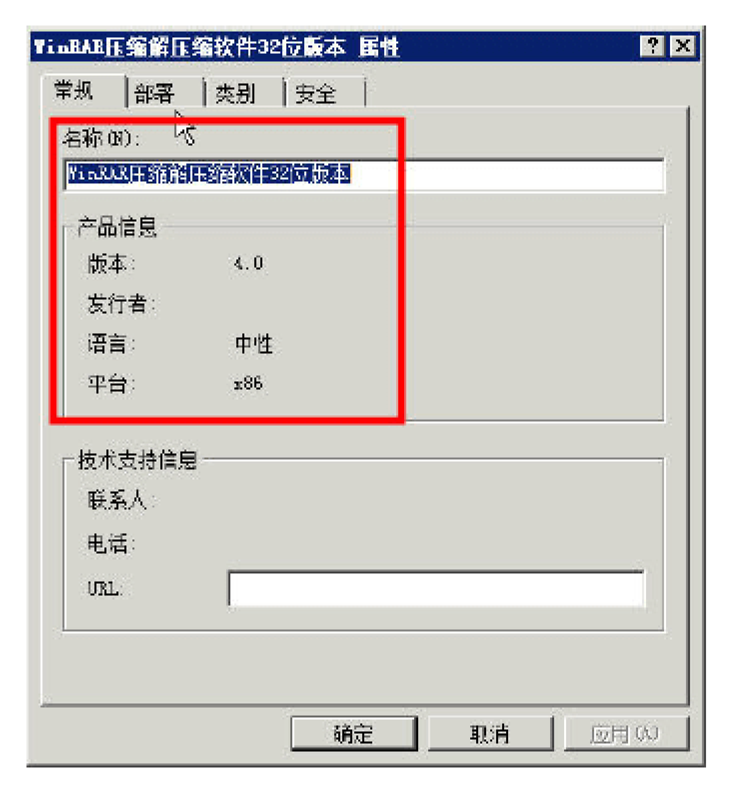


图 8-107　常规选项卡

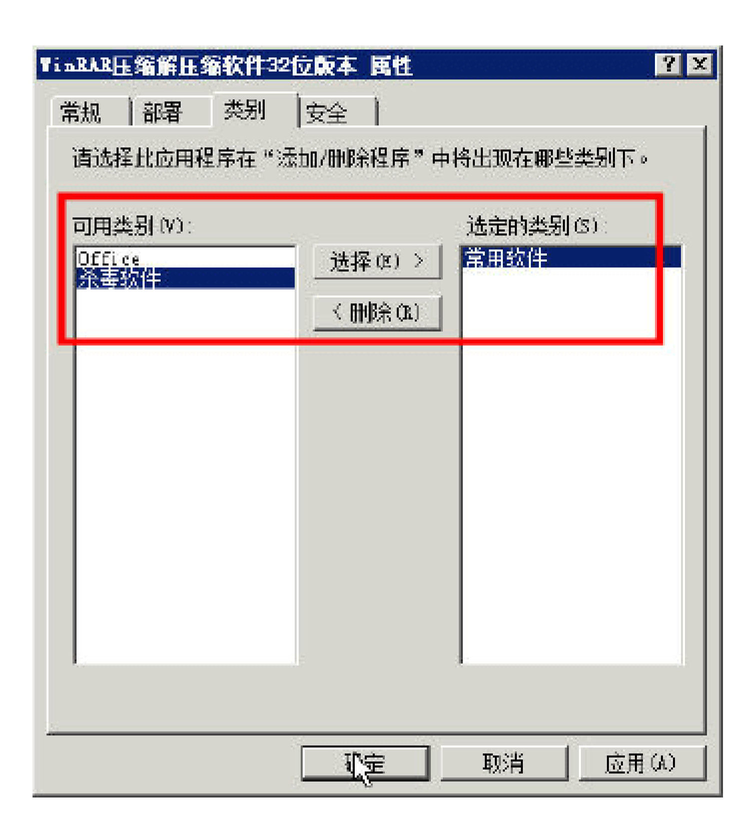


图 8-108　软件类别

设置之后，单击“确定”按钮返回。

11 如果要删除发布的软件包，可以单击鼠标右键，在弹出的对话框中选择“所有任务→删除”选项（如图 8-109 所示），并根据提示操作即可。

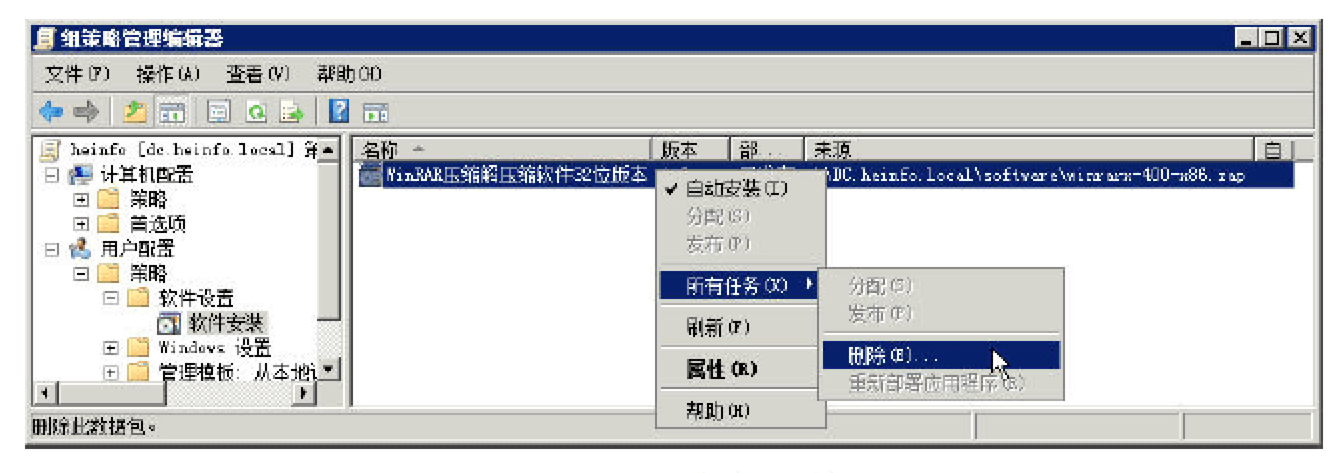


图 8-109　删除软件包

8.5.3　发布 Office 2003

现在许多单位仍然在使用 Office 2003，本小节介绍使用组策略发布 Office 2003 的方法，主要步骤如下：

- 为 Office 2003 启用“管理员安装”。
- 集成 Office 2003 的 SP3 到管理员安装目录。
- 使用组策略分发 Office 2003。

下面介绍详细的步骤。

01 将 Office 2003 安装光盘（或使用光盘镜像，用虚拟光驱加载光盘镜像）放入光驱，单击“开始”→“运行”命令，打开“运行”对话框。单击“浏览”按钮选择 Office 2003 的 setup.exe 程序，然后在后面加上空格及/a 参数，如图 8-110 所示。

02 在“Microsoft Office 2003 安装”窗口中，在“单位”文本框中输入单位名称，在“安装

位置”文本框中设置将要保存 Office 安装程序的路径（在本例为 E:\software\Office 2003），在“产品密钥”文本框中输入产品的安装序列号，如图 8-111 所示。

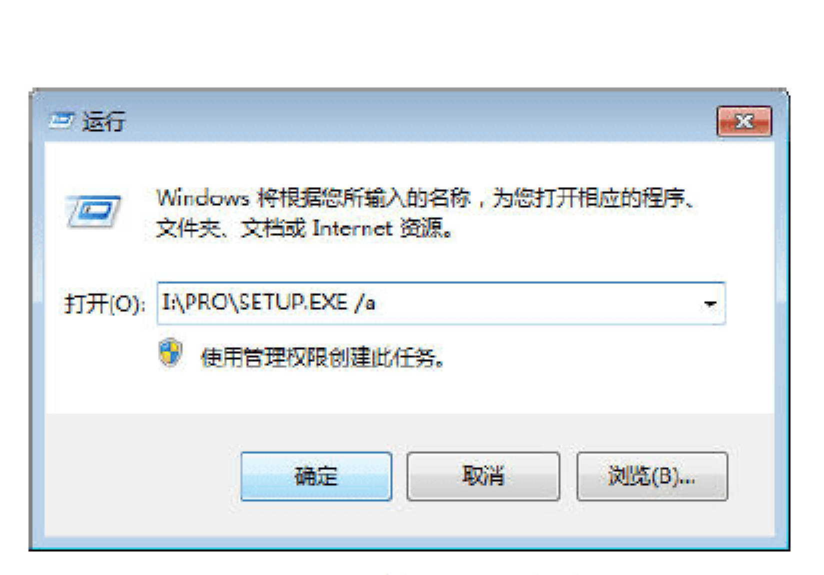


图 8-110　管理员安装

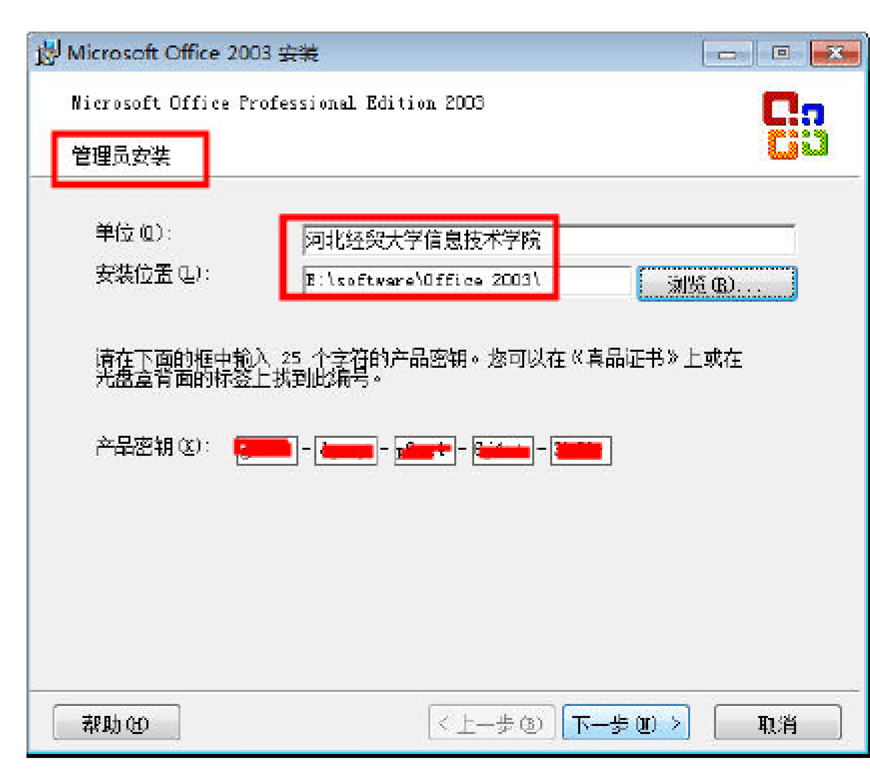


图 8-111　安装路径及产品序列号

03 在“最终用户许可协议”窗口，选中“我接受许可协议中的条款”复选框，单击“安装”按钮即可开始复制程序，如图 8-112 所示。复制文件之后，管理员安装完成，如图 8-113 所示。

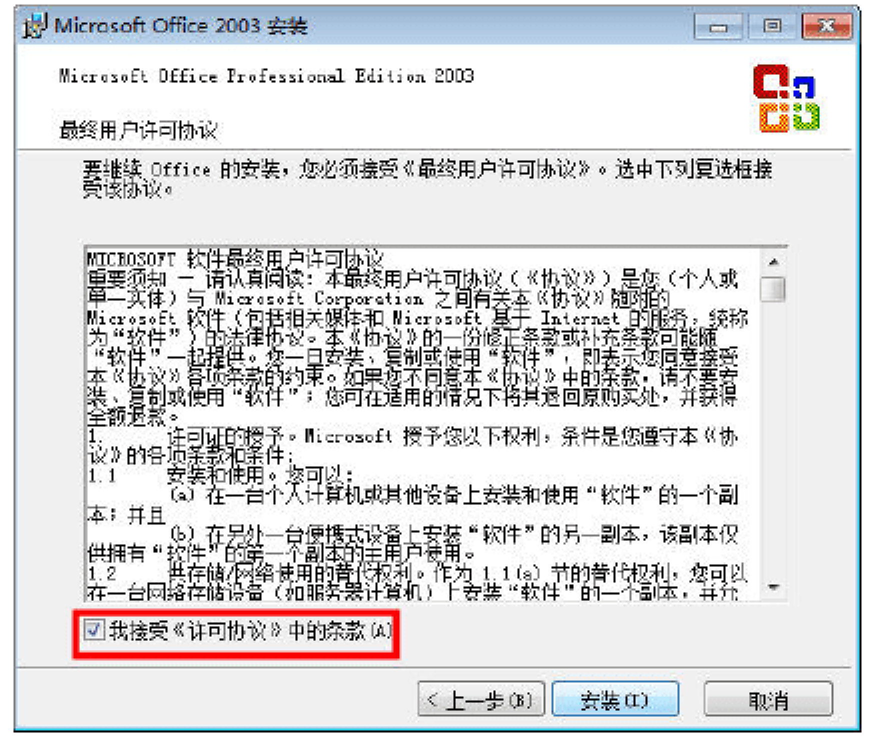


图 8-112　接受许可协议

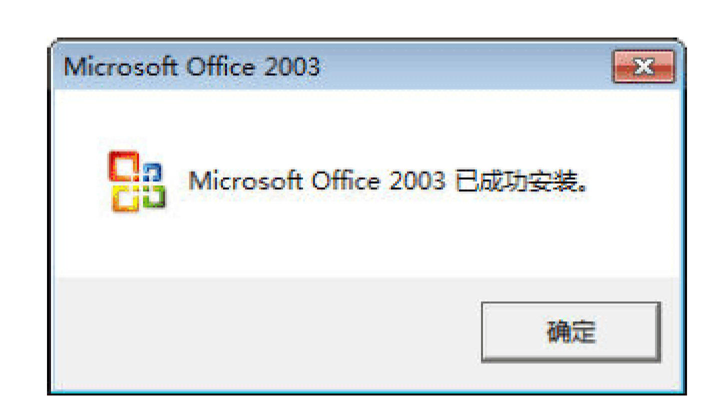


图 8-113　管理员安装完成

04 然后下载 Office SP3，下载之后，将其复制到 E 盘根目录，用鼠标单击右键，在弹出的快捷菜单中选择“解压到 Office2003SP3-KB923618-FullFile-CHS”选项，如图 8-114 所示。

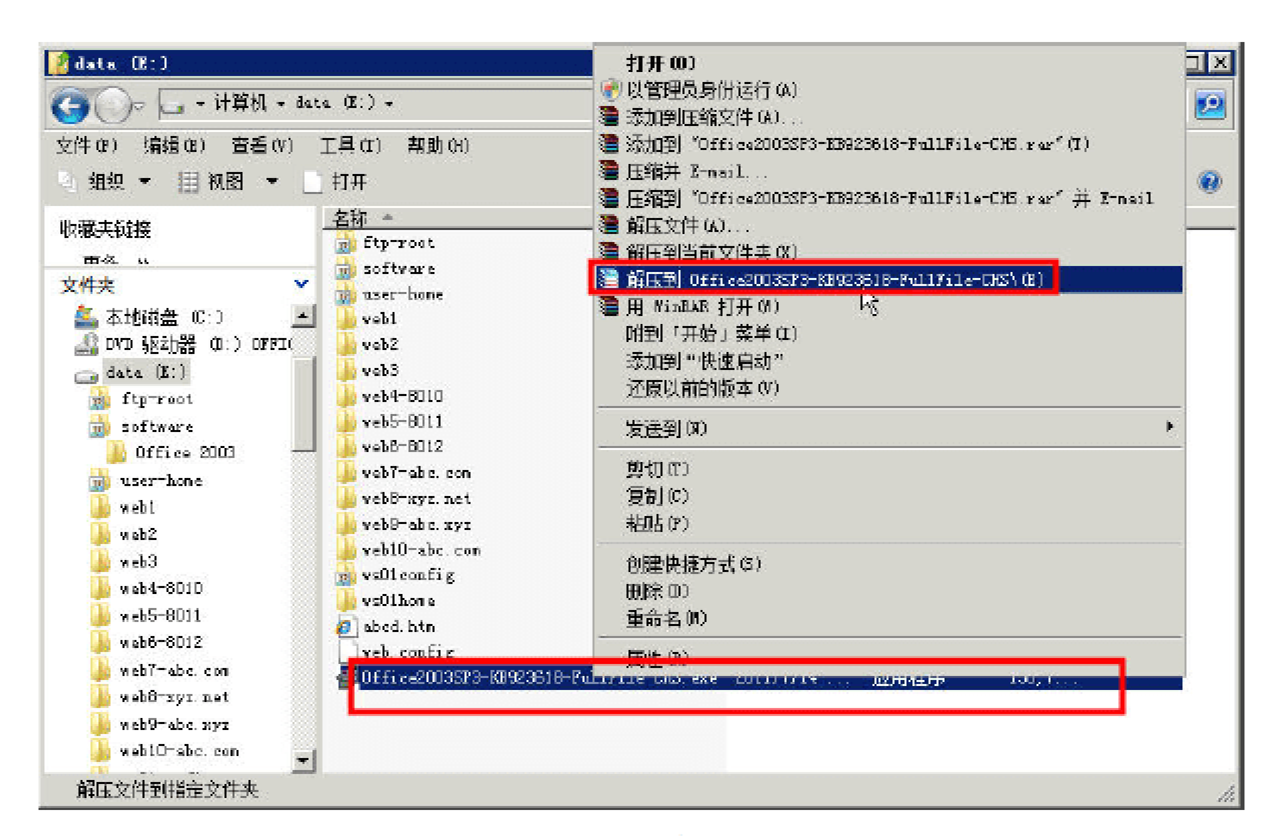


图 8-114　解压缩 Office 2003

05 解压缩后，打开 E 盘“Office2003SP3-KB923618-FullFile-CHS”文件夹，看到 Office 2003 SP3 的补丁文件，如图 8-115 所示。

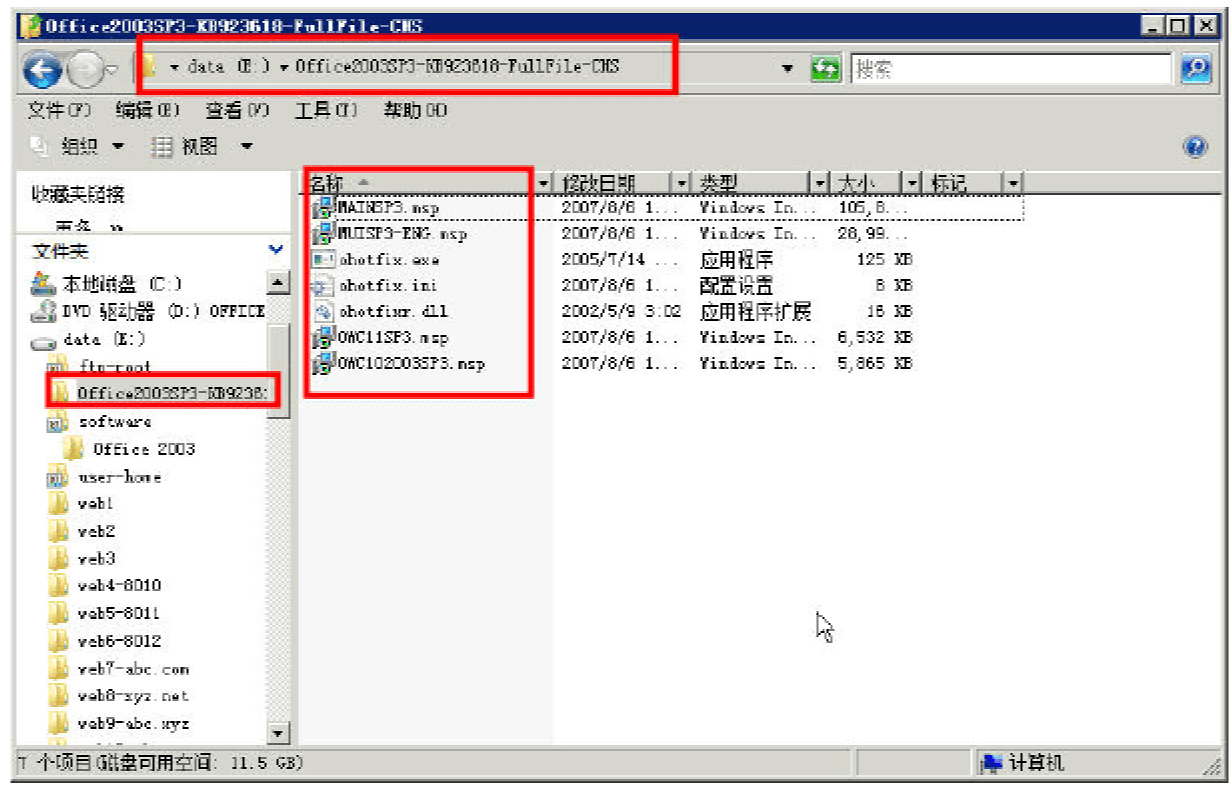


图 8-115　Office 2003 SP3 的补丁文件

06 然后进入命令提示符，进入 E 盘 Office2003SP3-KB923618-FullFile-CHS 文件夹，执行 mainsp3.msp /a "E:\software\Office 2003\pro11.msi"命令，如图 8-116 所示。

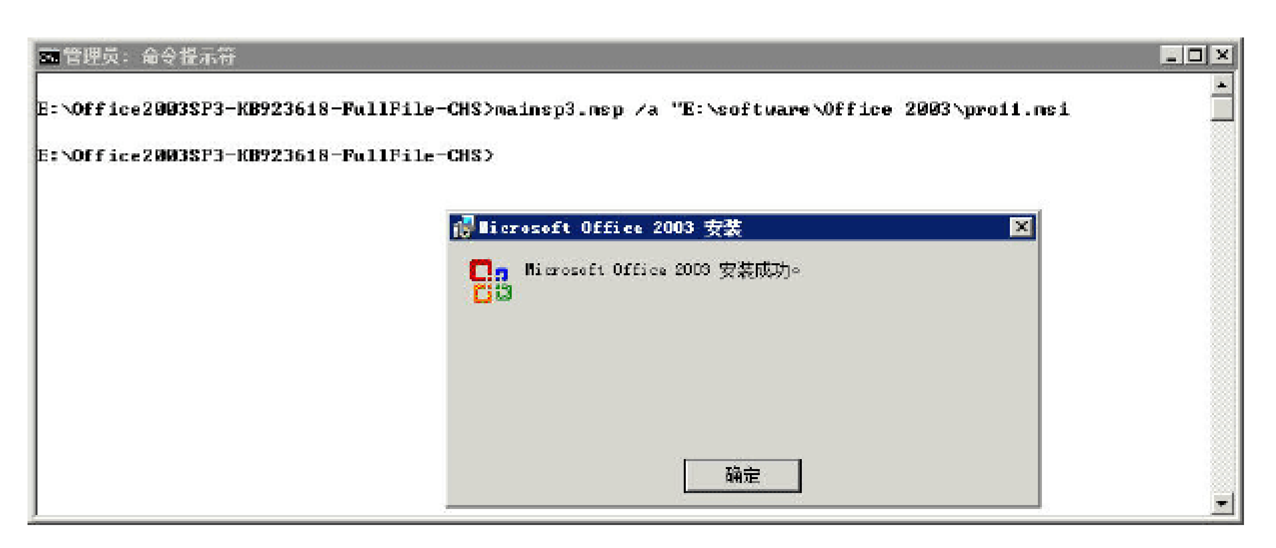


图 8-116　集成补丁到 Office 2003 的管理员安装目录

07 然后再执行 owc11sp3.msp /a "E:\software\Office 2003\owc11.msi"命令，在出现的“Microsoft Office Web Components”对话框中，接受许可协议（如图 8-117 所示），直接更新安装，如图 8-118 所示。





图 8-117　接受许可协议　　　图 8-118　集成 SP3

08 返回到“组策略编辑管理器”窗口，定位到“用户配置→策略→软件设置→软件安装”，

在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“新建→数据包”选项，如图 8-119 所示。

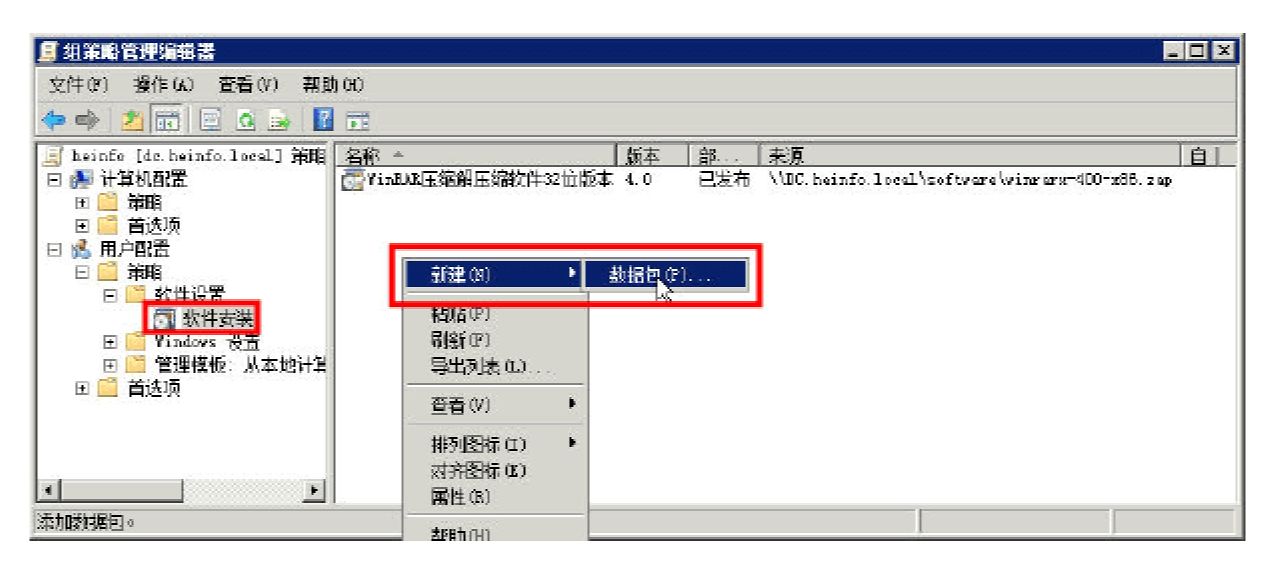
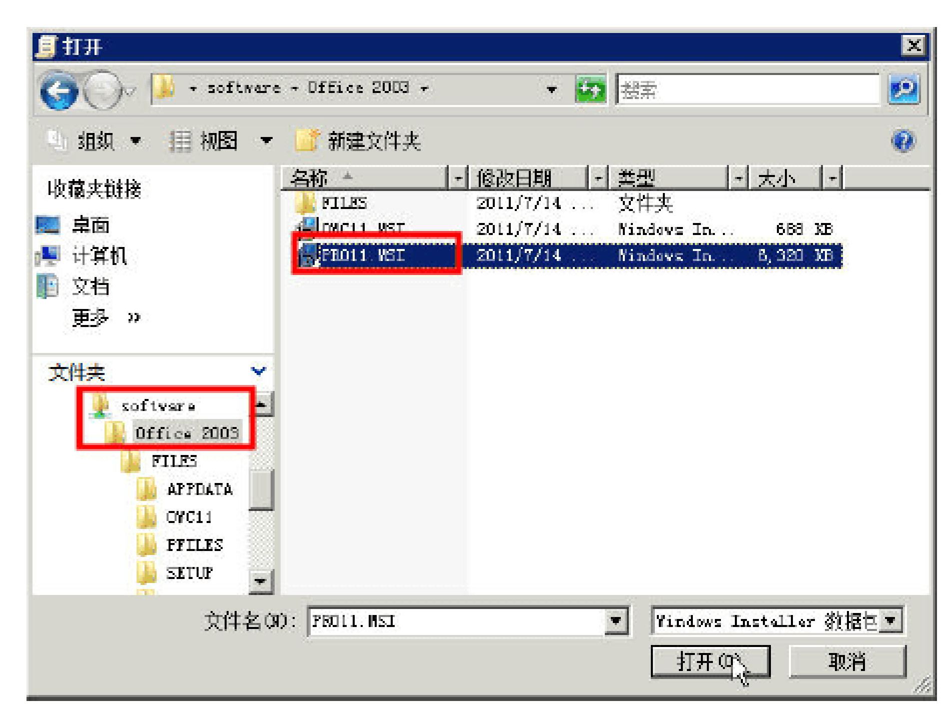


图 8-119　新建数据包

09 在“打开”对话框中，浏览到\\dc.heinfo.local\software\office 2003 文件夹，选中 PRO11.MSI，如图 8-120 所示。

10 在“部署软件”对话框中，选中“高级”单选按钮，如图 8-121 所示，单击“确定”按钮。



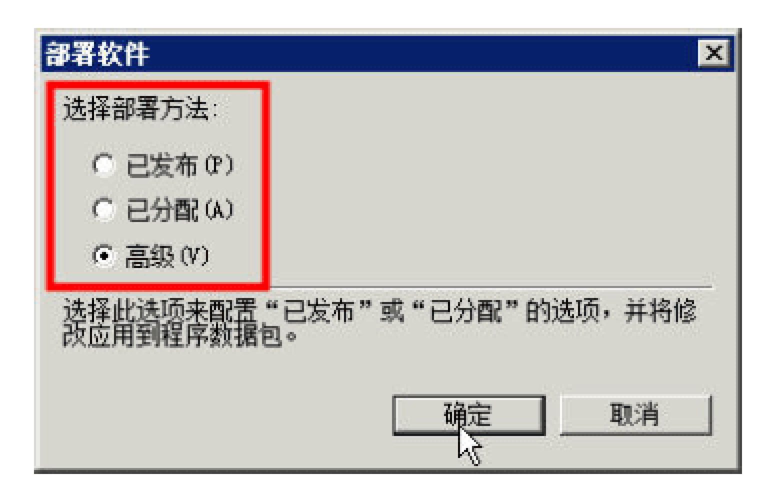


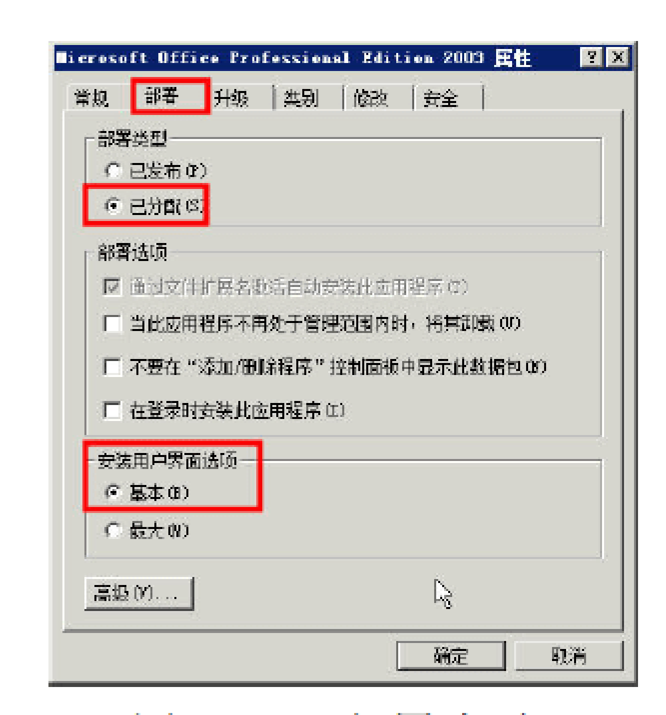
图 8-120　选择 Office 2003 安装程序　　图 8-121　选择部署方法

说 明

在图 8-121 中，已发布：指针对用户有效；已分配：对用户和计算机都有效。高级：指高级发布与高级分配。

11 在“部署”选项卡中，选择“已分配”与“基本”选项，如图 8-122 所示。

12 在“类别”选项卡中，选择“Office”，如图 8-123 所示。然后单击“确定”按钮，完成 Office 2003 的组策略分发工作。



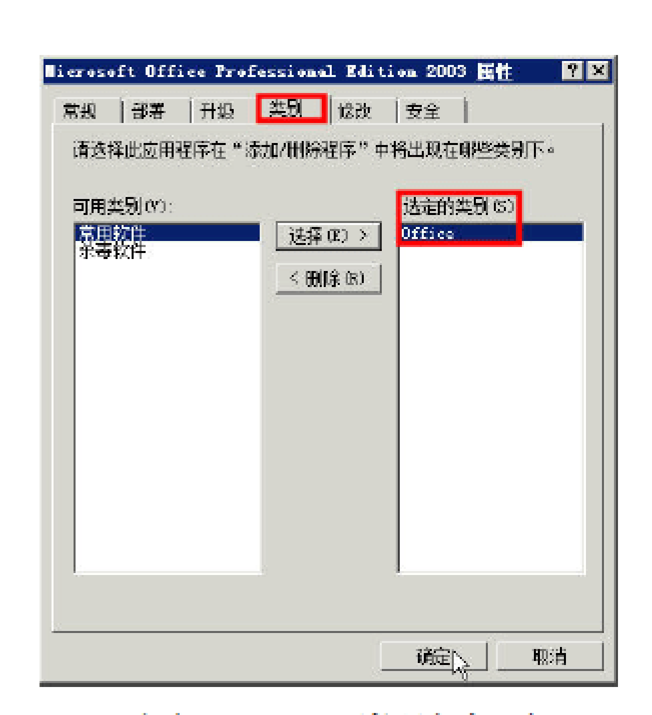
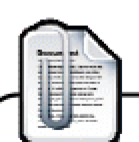


图 8-122　部署选项　　图 8-123　类别选项



说 明

在执行图 8-111 的时候，如果一直出现“在安装程序确定您的磁盘空间需求时，请耐心等待”（如图 8-124 所示），则退出安装程序，在另外一台机器上，执行“管理员安装”，在安装完成后，将管理员安装后的文件夹复制到服务器即可。



图 8-124　一直停留在该界面

8.5.4　深刻理解使用组策略定制软件

使用“组策略”发布软件，可以针对“计算机”和“用户”进行。这两者的区别如下：

- 如果在“计算机”对象上发布软件，将作用于 Active Directory 中的每一台计算机上，此时应该在 Active Directory 的“根”容器或“根 OU”上创建或修改组策略。在“计算机”上发布软件，主要用于系统的升级，而不是针对“用户”所做的设置。例如，在“计算机”对象上发布 Windows XP SP2 或 Windows Vista SP1 的补丁，此时，不管在计算机上登录的用户是使用哪个 OU 下的，都会生效。
- 如果在“用户”对象上发布软件，将作用于所属 OU 下的用户，而不是针对某台计算机。只要用户在某台计算机上登录，则作用于用户的组策略将在所属计算机上生效。

使用“组策略”发布软件时，可以发布 MSI 程序和 EXE 程序，其中 EXE 程序要创建一个 ZAP 包。这两种的区别是：MSI 程序可以发布、也可以分配，而 ZAP 包只能发布，不能分配。发布和分配的区别是：

- 发布的软件，只能通过用户在“添加/删除程序”中的“添加新程序”中添加，不能自动安装在用户的计算机中。
- 分配的软件，是在用户登录的时候，由系统自动安装，不需要用户自行添加。当然，分配的软件也可以在“添加/删除程序”中添加或删除。
- 发布的软件，用户可以根据需要添加或删除；而分配的软件，如果用户删除，则用户下次登录时，还是会自行添加。

对于“计算机”对象，只能使用“分配”的方法，不能使用“发布”的方法。也就是说，在“计算机”对象中只能部署 MSI 的程序包。在“计算机”对象部署 MSI 程序包的方法与在“用户”对象部署的方法类似。

8.6　使用组策略与脚本发布 Office 2010 到计算机

在前面使用组策略发布 EXE 与 Office 2003 时，是在“用户配置→策略→软件设置”中进行发布的，接下来我们介绍使用组策略与脚本分发 Office 2010 的办法，主要步骤如下。

01 为分发 Office 2010 创建两个共享文件夹，一个文件夹保存 Office 2010 的安装程序，此共享为所有用户设置“只读”权限；另一个文件夹保存安装 Office 2010 的日志，此文件夹需要让所有用户具备“读写”权限。

02 下载 Office 2010 的管理员工具及脚本，为安装 Office 2010 进行自定义设置。

03 为分发 Office 2010 创建 OU，并编写 Office 2010 的安装脚本，自定义用户使用 Office 2010 的策略。

04 在客户端测试。

在接下来的内容中，将详细介绍上述每一步操作。

8.6.1　准备 Office 2010 安装程序

在使用组策略发布 Office 2010 的时候，可以使用以前创建的 software 的共享文件夹，用户可以在该文件夹中创建一个 Office2010 的文件夹（注意，不要有空格），将 Office 2010 安装光盘中的所有文件及文件夹复制到该文件夹，如图 8-125 所示。注意，Office 2010 分 32 位与 64 位版本，本书以 32 位版本为例。

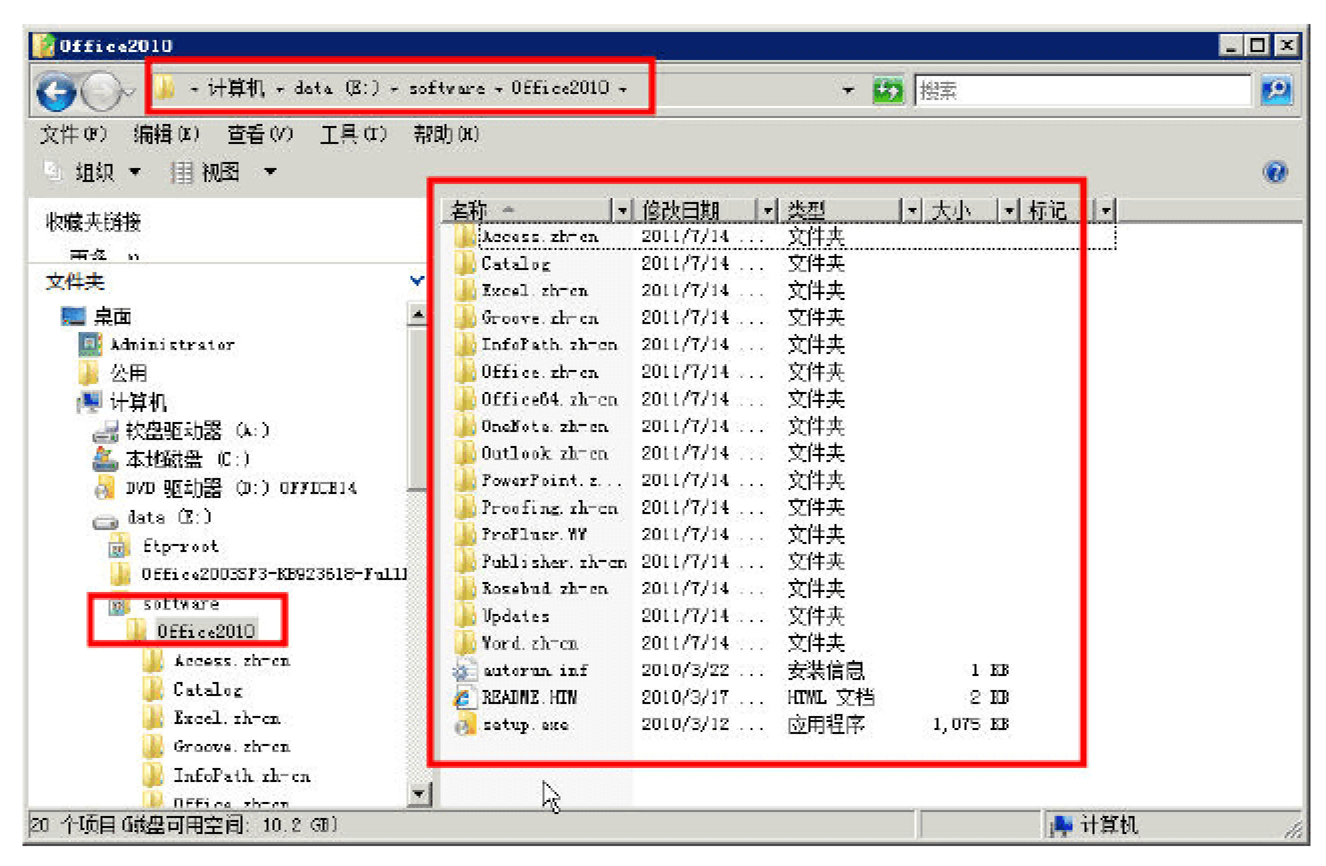


图 8-125　复制 Office 2010 安装文件

然后从 http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=18968 站点下载“Office 2010 Administrative Template files（ADM, ADMX/ADML）and Office Customization Tool”，该程序同样有 32 位与 64 位版本，32 位版本名为 AdminTemplates_32bit.exe，64 位版本名为 AdminTemplates_64bit.exe，大小都是 15MB，如图 8-126 所示。可根据需要分发的 Office 2010 选择对应的版本，在本例中，选择 32 位的 Office 2010 自定义工具。

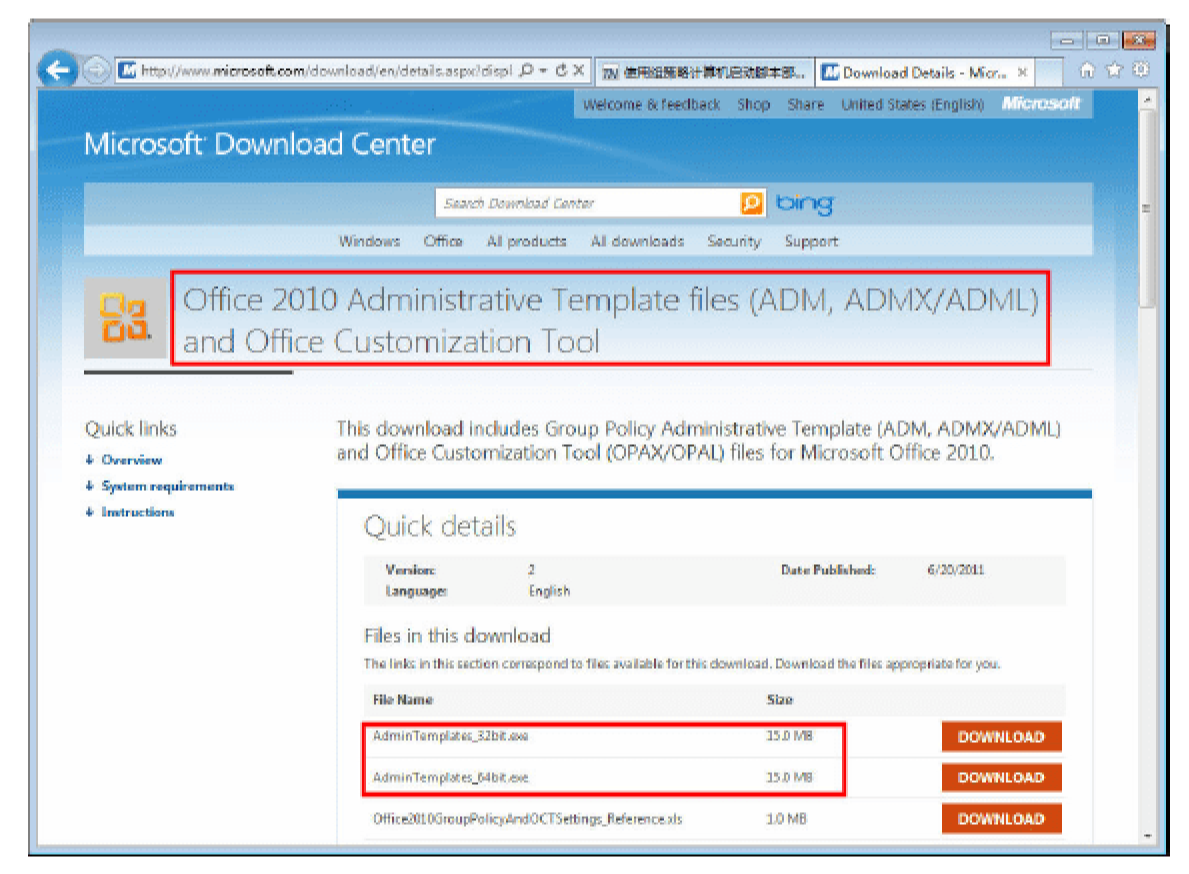


图 8-126　下载 Office 2010 管理员模板文件与自定义工具

在下载 Office 2010 模板文件与自定义工具后，运行该程序，接受许可协议（如图 8-127 所示），然后选择一个文件夹（如图 8-128 所示），Office 2010 管理模板文件与自定义工具将会解压缩到该文件夹。

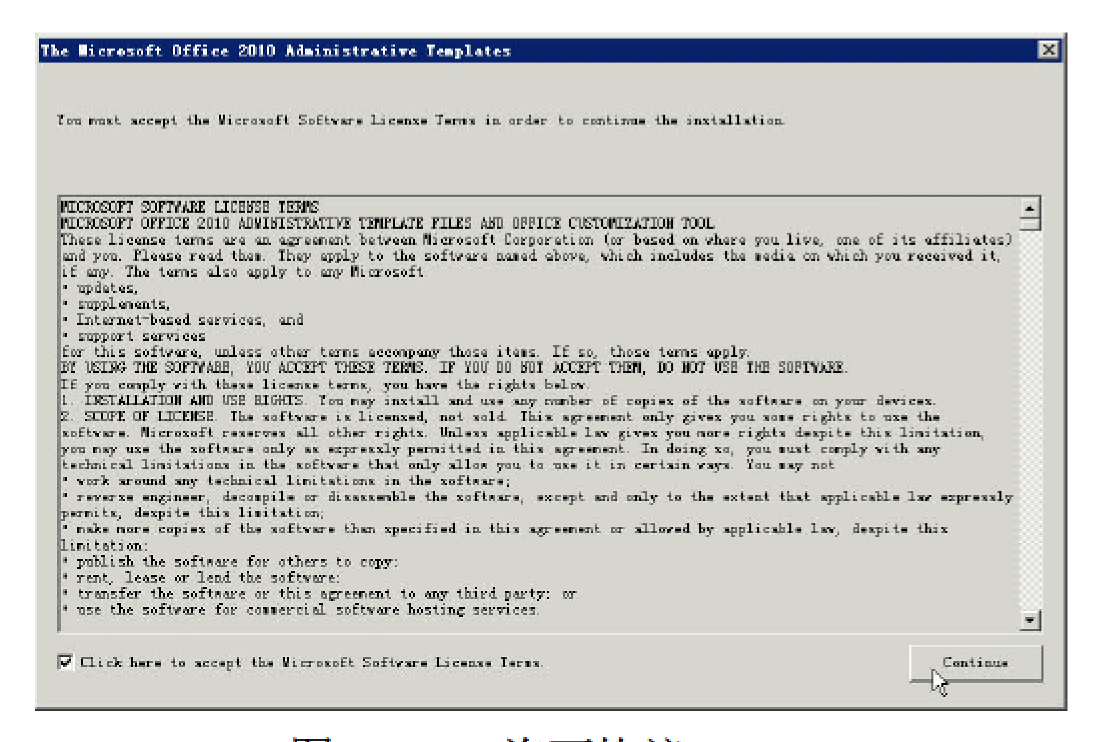
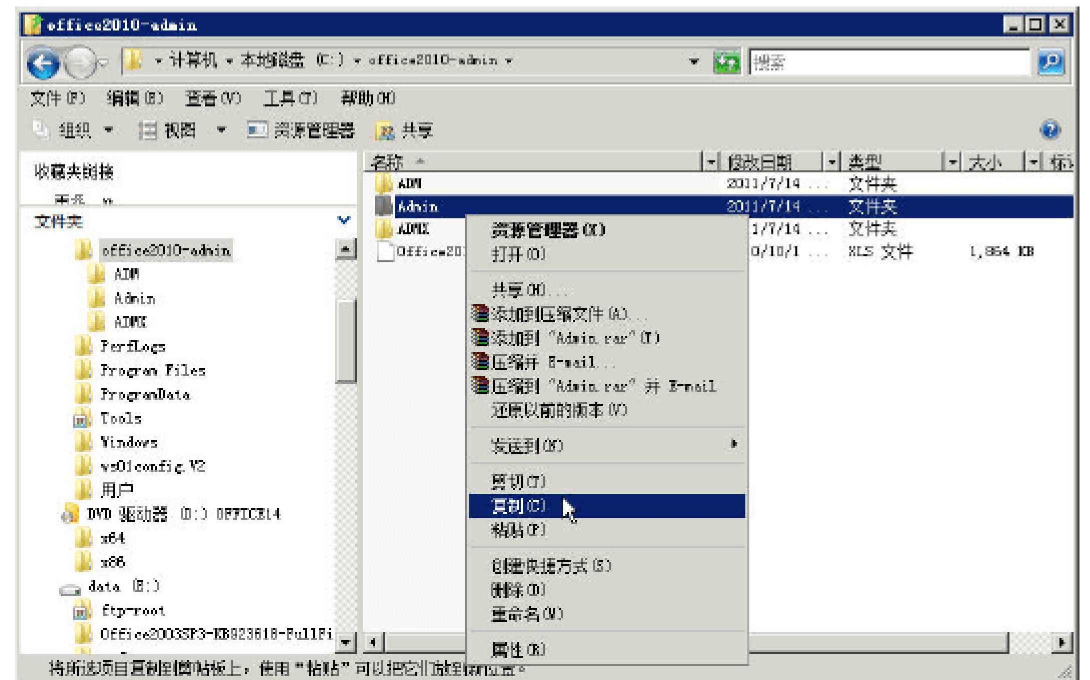


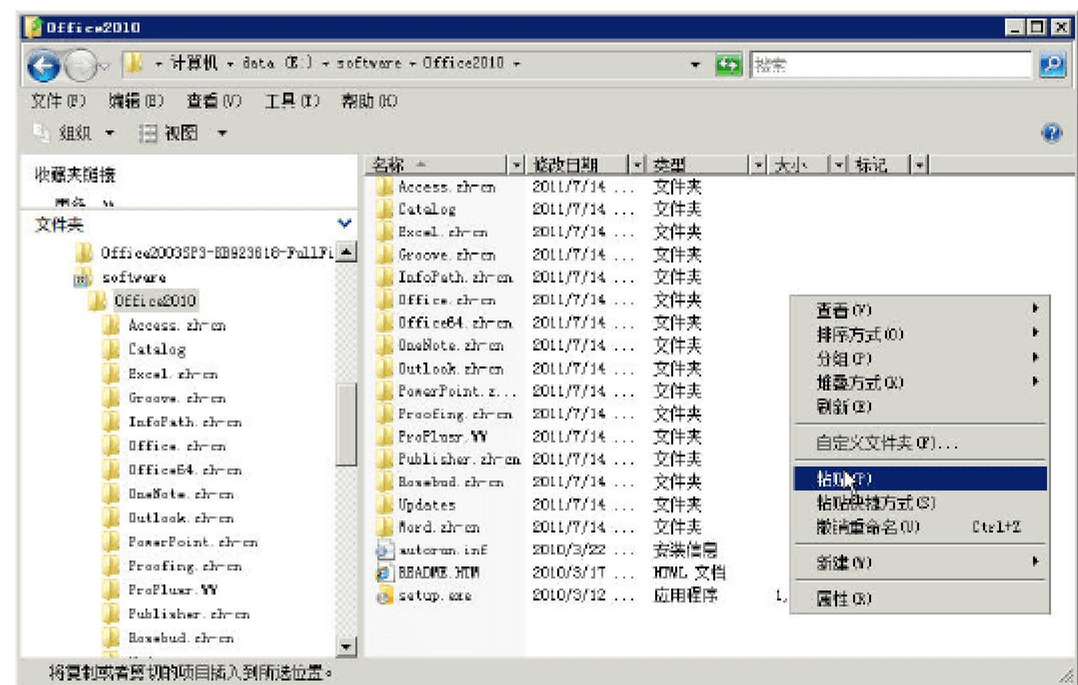
图 8-127　许可协议



图 8-128　选择解压缩的文件夹

在解压缩之后，打开图 8-128 中指定的文件夹，将其中的 Admin 文件夹（如图 8-129 所示）复制到图 8-125 中的 Office 2010 安装程序所在的目录，如图 8-130 所示。


图 8-129　复制 Admin 文件夹


图 8-130　粘贴到 Office 2010 安装程序路径

8.6.2　Office 2010 自定义文件

在准备好 Office 2010 安装程序及 admin 文件夹后，运行 Office 2010 的自定义程序，为安装 Office 2010 进行自定义，主要步骤如下。

01 运行命令提示符，进入 Office 2010 所在的目录，执行“setup /admin”命令，如图 8-131 所示。

02 打开“Microsoft Office 自定义工具”，选择“新建用于下列产品的安装程序自定义文件”选项，并单击“确定”按钮，如图 8-132 所示。

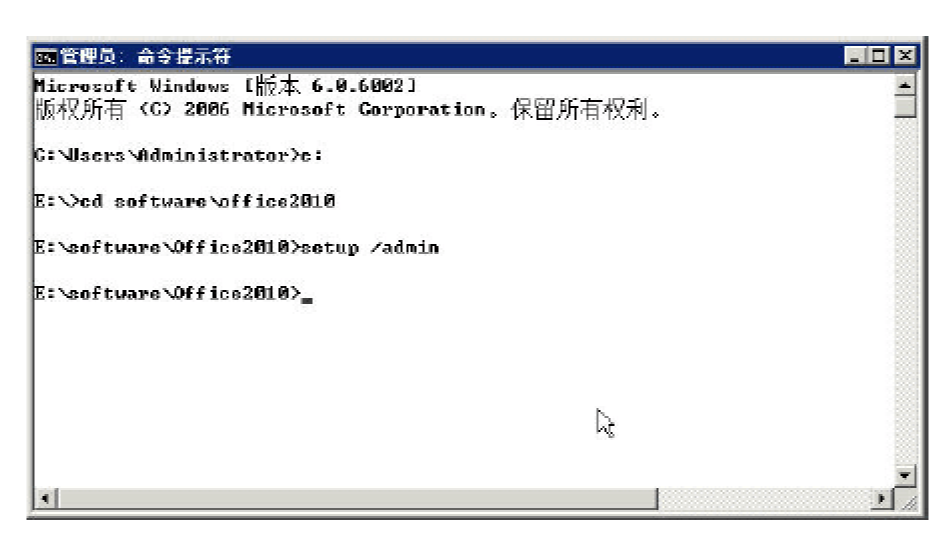


图 8-131　运行 setup /admin

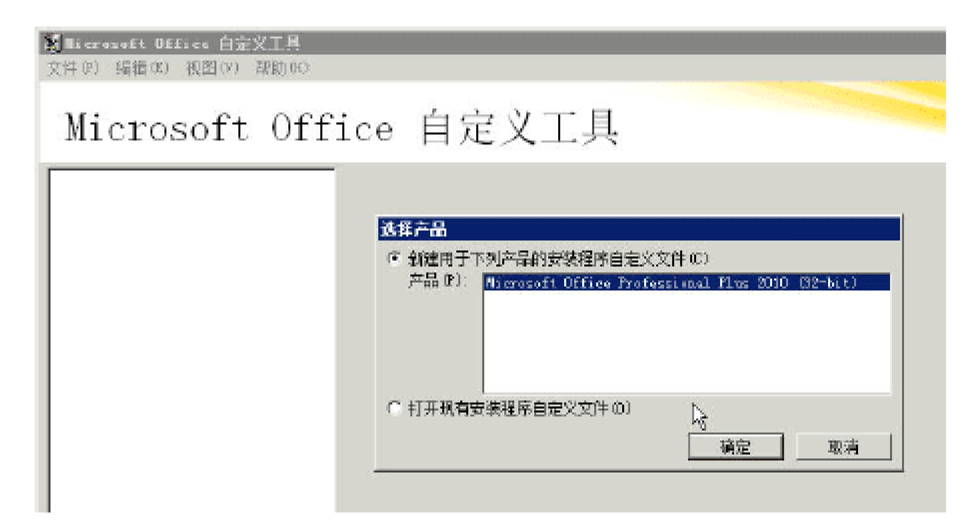


图 8-132　运行 Microsoft Office 自定义工具

说 明

如果是第一次使用 Microsoft Office 自定义工具，一定要选择“新建用于下列产品的安装程序自定义文件”选项，此时自定义工具将会从当前的 Office 2010 安装程序中提取配置。由于 Office 2010 有多个产品与多个版本，例如有 VL 版本（不需要输入序列号、使用 KMS 服务器激活的），有普通的需要输入序列号激活的产品，还有 32 位与 64 位版本。所以，在使用自定义工具的时候，一定要将所要分发的 Office 2010 复制到服务器中，并将 admin 文件复制到 Office 2010 的安装目录中，同时配套使用才可以。只有使用图 8-132 新建用于下列产品的安装程序自定义文件（读取当前产品配置），根据以后的步骤修改配置并保存之后，才可以选择“打开现有安装程序自定义文件”选项并再次修改，但不能打开用于其他产品、版本的自定义文件。

03 Office 2010 自定义工具中的配置比较多，我们只介绍主要的几种。在“安装位置和单位名称”选项中，可以输入“单位名称”，如图 8-133 所示。

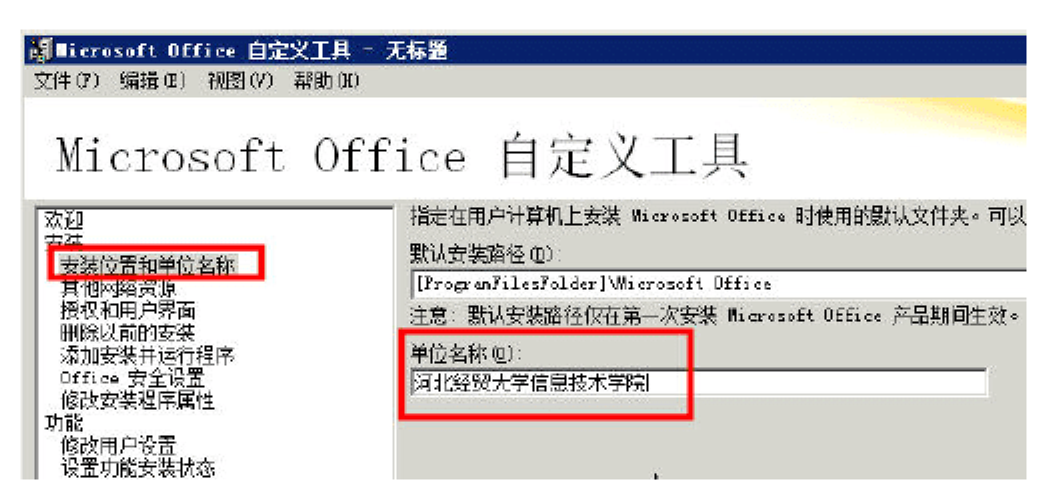


图 8-133　单位名称

04 在“授权和用户界面”窗格中，设置 Office 2010 的产品密钥，或者选择使用 KMS 客户端密钥（将用 KMS 对 Office 2010 进行激活）选项，如图 8-134 所示。如果当前的 Office 2010 是 VL 版本，须选择“使用 KMS 客户端密钥”选项；如果当前的产品是使用序列号激活的，须选择

“输入其他产品密钥”选项并输入用于当前 Office 产品的序列号。如果用于企业部署，且要输入序列号，应输入可用于多次激活的 MAK 的序列号。

选中“我授受《许可协议》中的条款”复选框。在 “显示级别”下拉列表中，有 3 项选择，分别是“无、基本、完全-默认”。如果选择“无”，则使用该自定义文件时，在安装的过程中没有任何的显示；如果选择“基本”，在安装的过程中，会显示安装的界面，但不能选择；如果选择“完全-默认”，则在安装的过程中，除了会显示安装界面外，还会让用户选择安装的选项。由于 Office 2010 的安装过程比较“漫长”，所以，推荐在“显示级别”下拉列表中选择“基本”选项。如果想让 Office 安装程序安装完成后，提示“安装完成”，可以选中“完成通知”复选框，且如果不需要该通知，可以不必选择。

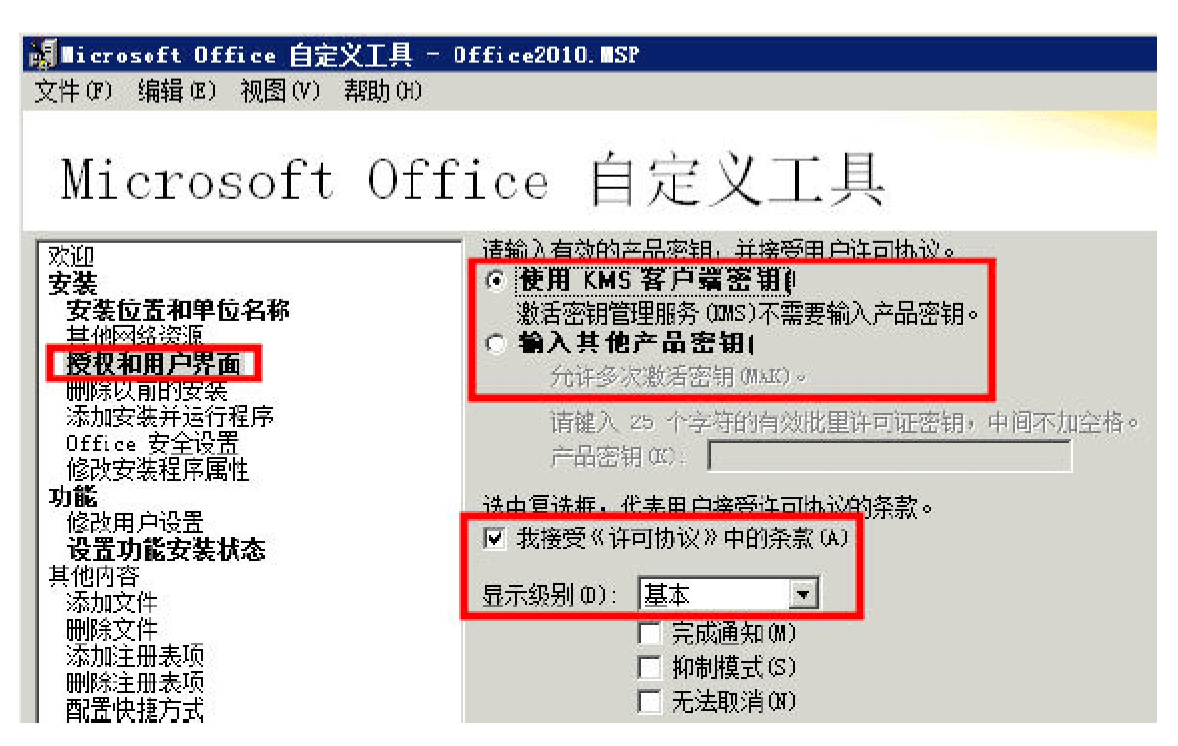
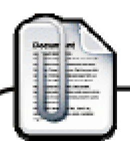


图 8-134　授权和用户界面



说 明

如果使用的是 VL 版本的 Office，则不能选择“输入其他产品密钥”选项，反之亦然。如果进行了错误的选择，则应用该配置文件时，会出现错误。本示例中，使用的是 Office 2010 的 VL 版本，所以选择“使用 KMS 客户端密钥”选项。

05 在“修改用户设置”窗口，可以自定义 Office 2010 中的每个产品的设置，如图 8-135 所示。通常使用默认值即可。

06 在“设置功能安装状态”窗口，自定义要安装的 Office 产品，如图 8-136 所示。用户可以单击每个产品并选择“从本机运行、从本机运行全部程序、在首次使用时安装、不可用”等选项。



图 8-135　修改用户设置

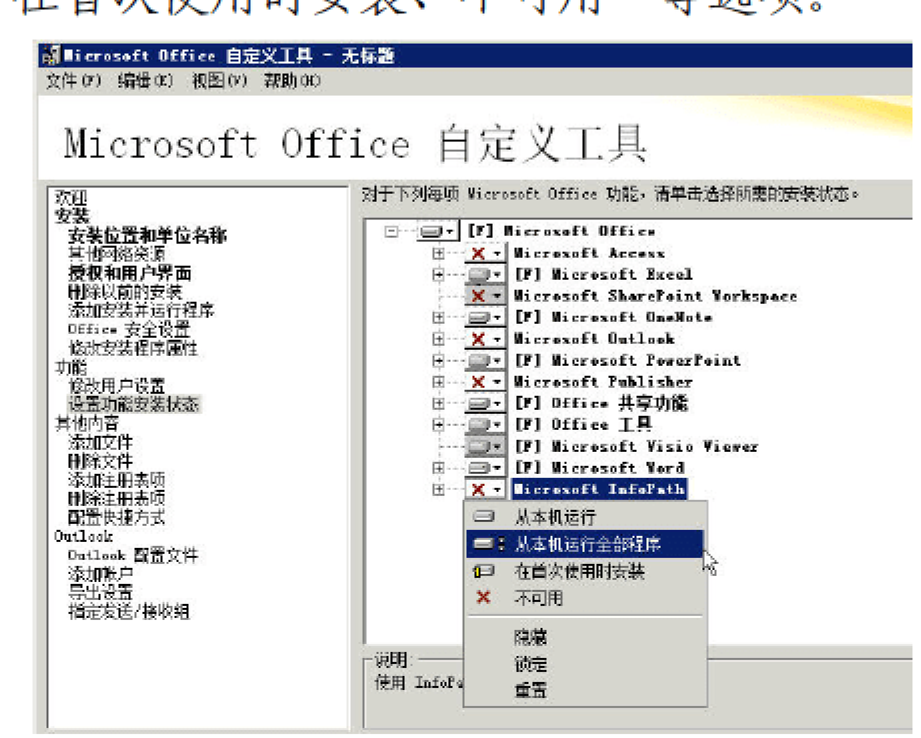


图 8-136　设置功能安装状态

07 其他设置可以保持默认值，或者根据需要做出设置。然后单击“文件”菜单选择“保存”菜单命令，如图 8-137 所示。

08 在弹出的“另存为”对话框中，将 Office 2010 的自定义文件保存到 Office 2010 安装程序所在的 Updates 文件夹中。注意，一定要是这个文件夹！而保存的文件名可以随意，例如设置为 Office2010Pro，系统将会自动保存为扩展名为 msp 的文件，如图 8-138 所示。



图 8-137　保存

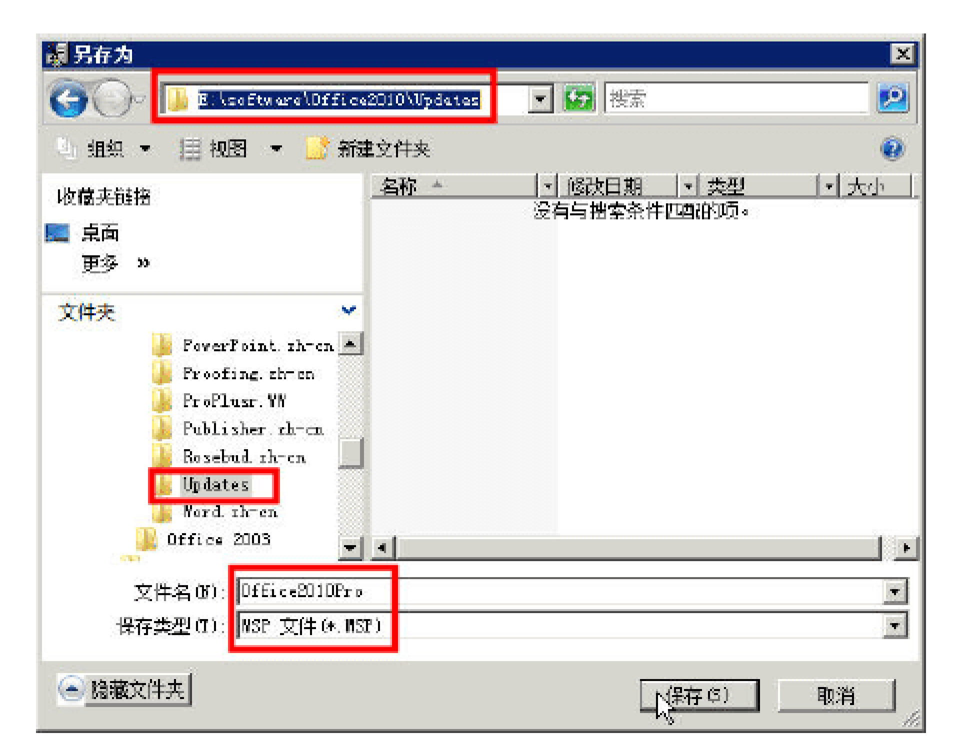
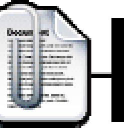


图 8-138　保存自定义文件到 updates 目录



说　明

自定义文件名任意，保存位置确定。在本示例中，自定义文件名为 office2010pro.msp，保存在 Office 2010 的 Updates 文件夹中。

如果要使用自定义文件进行测试，可以在服务器中，进入命令提示窗口，输入如下的命令进行测试：

```
e:
cd   \software\office2010
setup   /adminfile   updates\office2010pro.msp
```

如果配置文件无误，则会弹出“安装进度”对话框，显示 Office 2010 的安装过程，如图 8-139 所示。

如果自定义文件有问题，或者使用不正确的自定义文件，则会弹出“安装错误”的提示框，如图 8-140 所示，单击“确定”按钮，然后执行 setup /admin，可重新创建或修改自定义文件。

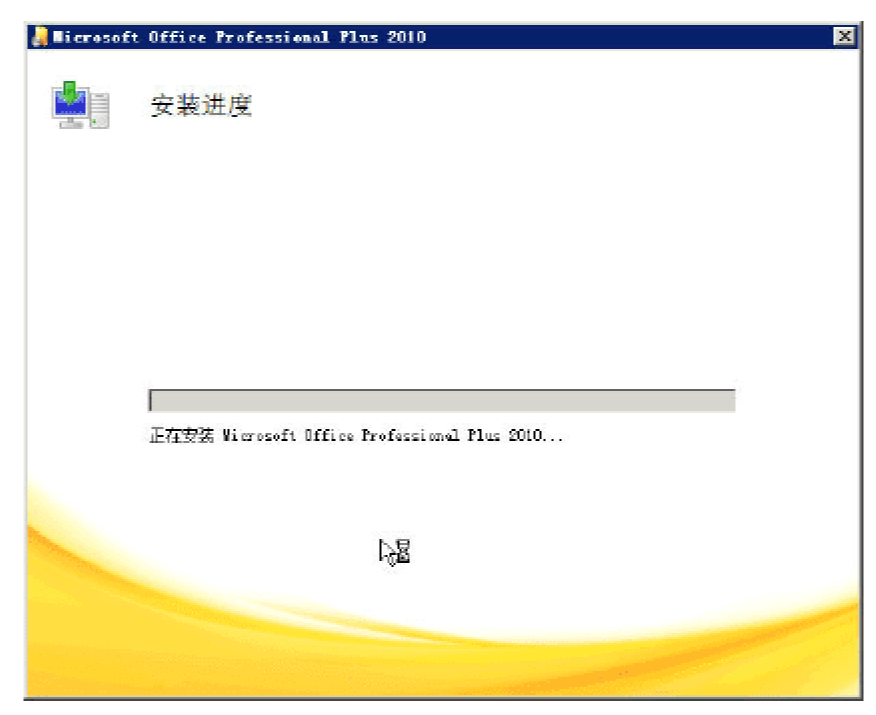


图 8-139　使用自定义文件安装 Office 2010

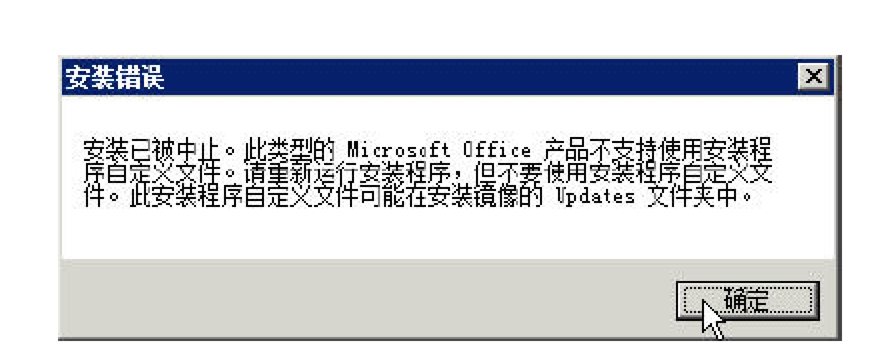


图 8-140　自定义文件不适合当前产品

8.6.3 修改 Office 2010 配置文件

如果不使用 8.6.2 小节中的“自定义工具”创建的自定义文件，而是使用默认的方式安装 Office 2010，也可以修改 Office 2010 的 config.xml 文件，步骤如下。

01 使用文本编辑器工具（例如记事本）打开所安装 Office 产品（本例中为 Office Professional Plus 2010）的 config.xml 文件。默认情况下，config.xml 文件位于核心产品 .WW 文件夹（本例中为 E:\software\Office2010\ProPlusr.WW）中。



说 明

在 Office 2010 的 VL 版本中，config.xml 的文件所在目录是 proplus.ww，而在其他版本中，文件目录是 proplusr.ww，大家要注意这一区别。

02 找到包含 Display 元素的行，如下面的示例所示：

```
<!-- <Display Level="full" CompletionNotice="yes" SuppressModal="no" AcceptEula="no" /> -->
```

删除注释分隔符“<!--”和“-->”，并修改为：

```
<Display Level="none" CompletionNotice="no" SuppressModal="yes" AcceptEula="yes" />
```

修改之后，如图 8-141 所示。

```
<Configuration Product="ProPlusr">
    <Display Level="none" CompletionNotice="no" SuppressModal="yes" AcceptEula="yes" />
    <!-- <Logging Type="standard" Path="%temp%" Template="Microsoft Office Professional Plus Se
    <!-- <USERNAME Value="Customer" /> -->
    <!-- <COMPANYNAME Value="MyCompany" /> -->
    <!-- <INSTALLLOCATION Value="%programfiles%\Microsoft Office" /> -->
```

图 8-141 修改 config.xml 文件

03 修改之后保存退出，并用鼠标双击，用 IE 浏览器打开该文件，内容显示如图 8-142 所示为正常。

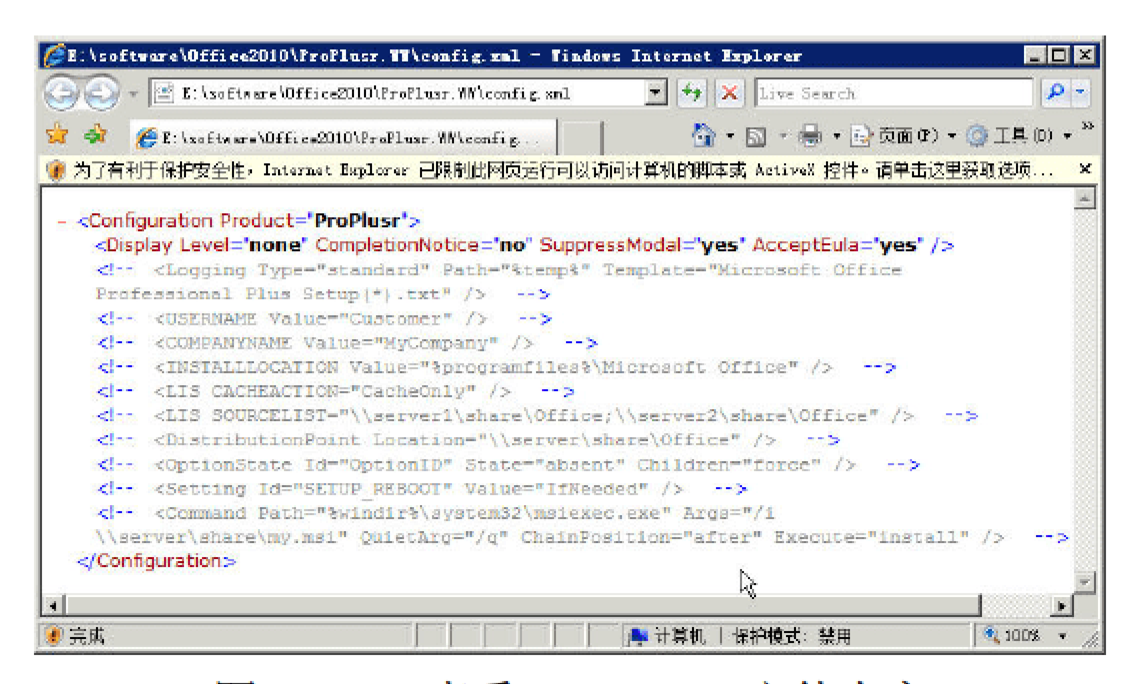


图 8-142 查看 config.xml 文件内容

04 如果修改的配置文件有问题，会在 IE 浏览器中显示，提示错误在第几行。如果出现错误，请重新用“记事本”打开 config.xml 并进行修改。建议在修改该文件前对该文件进行保存（例如保

存到另一位置，或用 winrar 对该文件进行压缩）。

如果要测试使用 config.xml 文件安装 Office，则执行如下的命令：

```
e:
cd    \software\office2010
setup.exe    /config    proplus.ww\config.xml
```

则安装程序会根据 config.xml 的内容自动完成安装。如果使用本示例所修改的配置文件，则在安装的过程中，屏幕上不会有任何显示，可以通过“任务管理器→进程”查看到 setup.exe 程序在运行，直到 Office 2010 安装完成，如图 8-143 所示。

如果以前在服务器上安装了 Office 2010，须进入“控制面板→程序和功能”中，将其卸载（如图 8-144 所示），等 Office 2010 卸载完成之后，再进行上述测试。

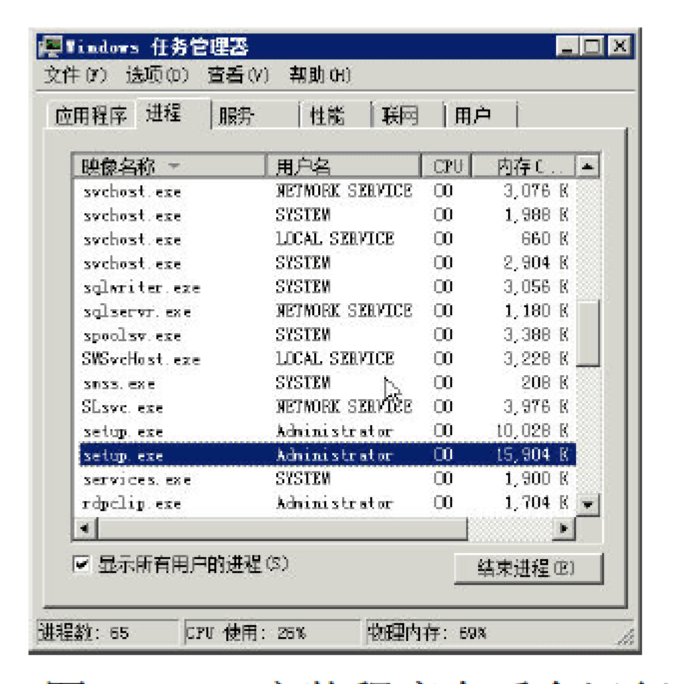


图 8-143　安装程序在后台运行

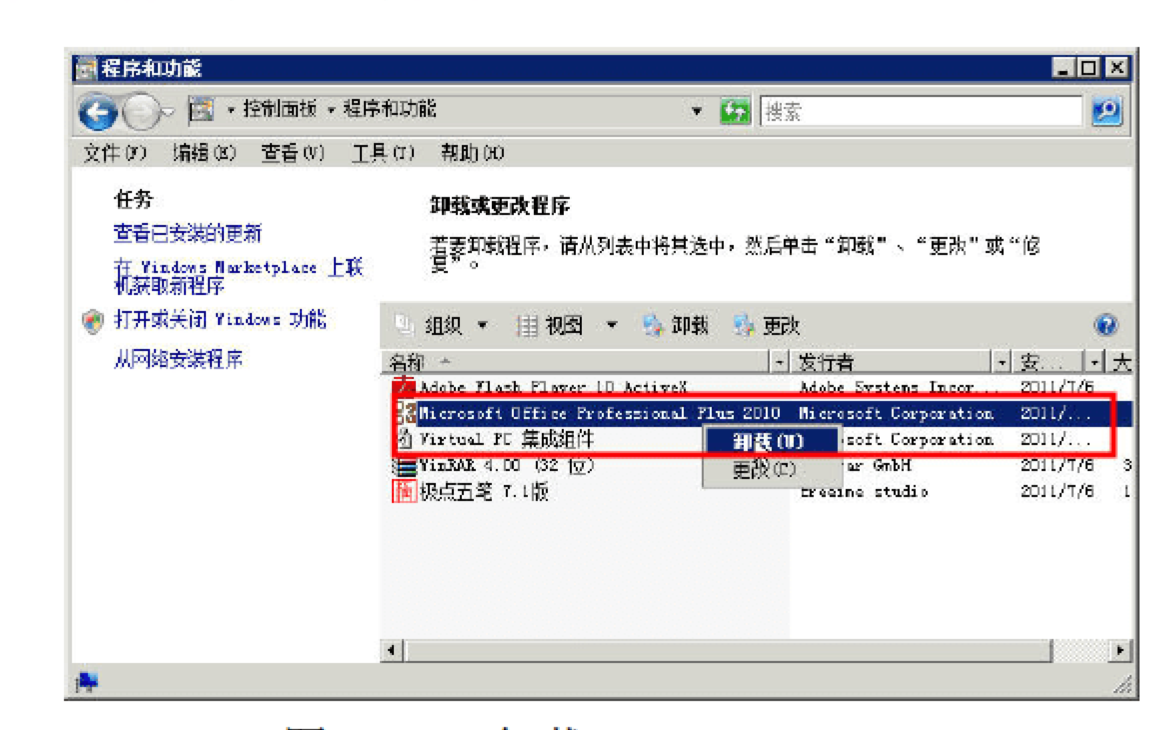


图 8-144　卸载 Office 2010

8.6.4　创建 OU 并编写脚本

在本小节中，要创建专门用来分发 Office 2010 的组织单位、编写脚本，步骤如下：

01 在服务器上创建 office2010Log 文件夹，并设置共享，允许 Everyone 用户组具有“完全控制”权限，如图 8-145 所示。

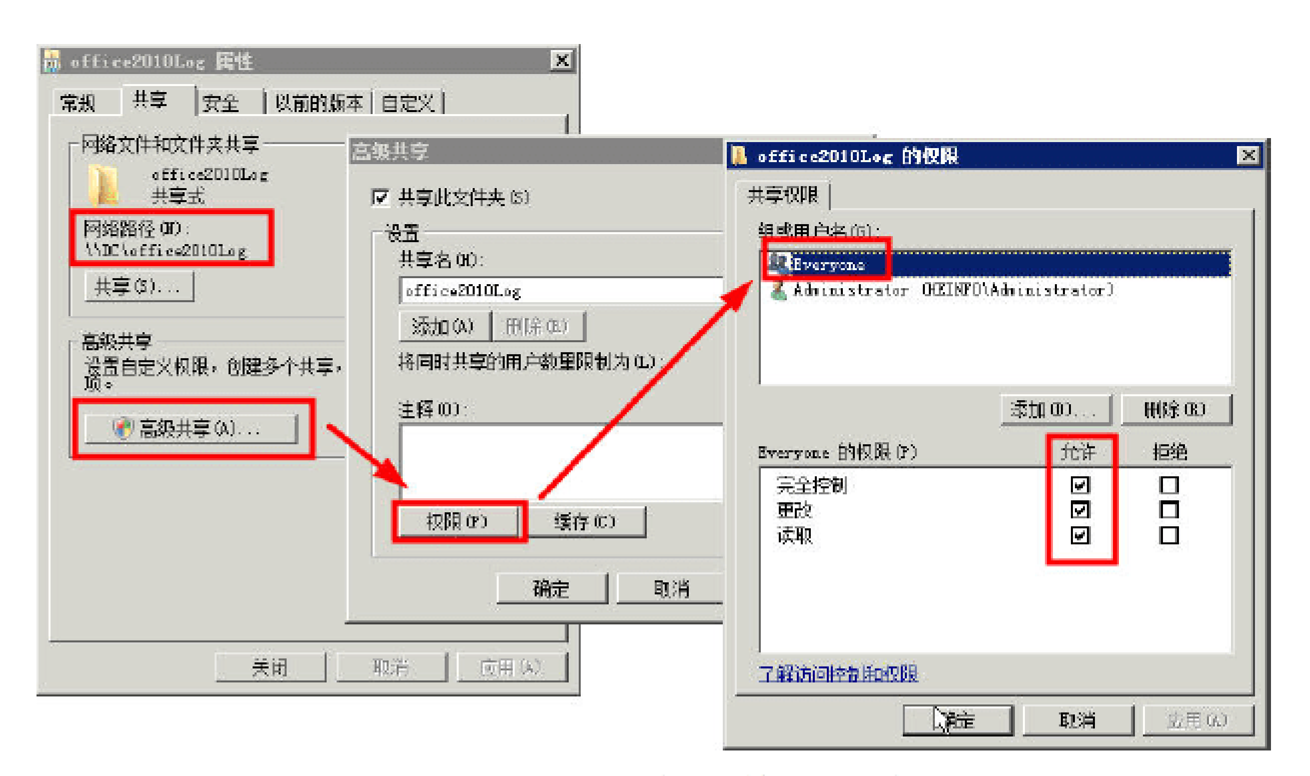


图 8-145　创建共享、修改共享权限

02 打开“服务器管理器”窗口，在“角色→Active Directory 域服务→Active Directory 用户和计算机”中创建一个组织单位，在此命名为“部署 Office 2010”，然后在“功能→组策略管理

→林→域→heinfo.local→部署 Office 2010”组织单位中创建组策略并编辑，在本例中，组策略名为 Deploy Office 2010，如图 8-146 所示。

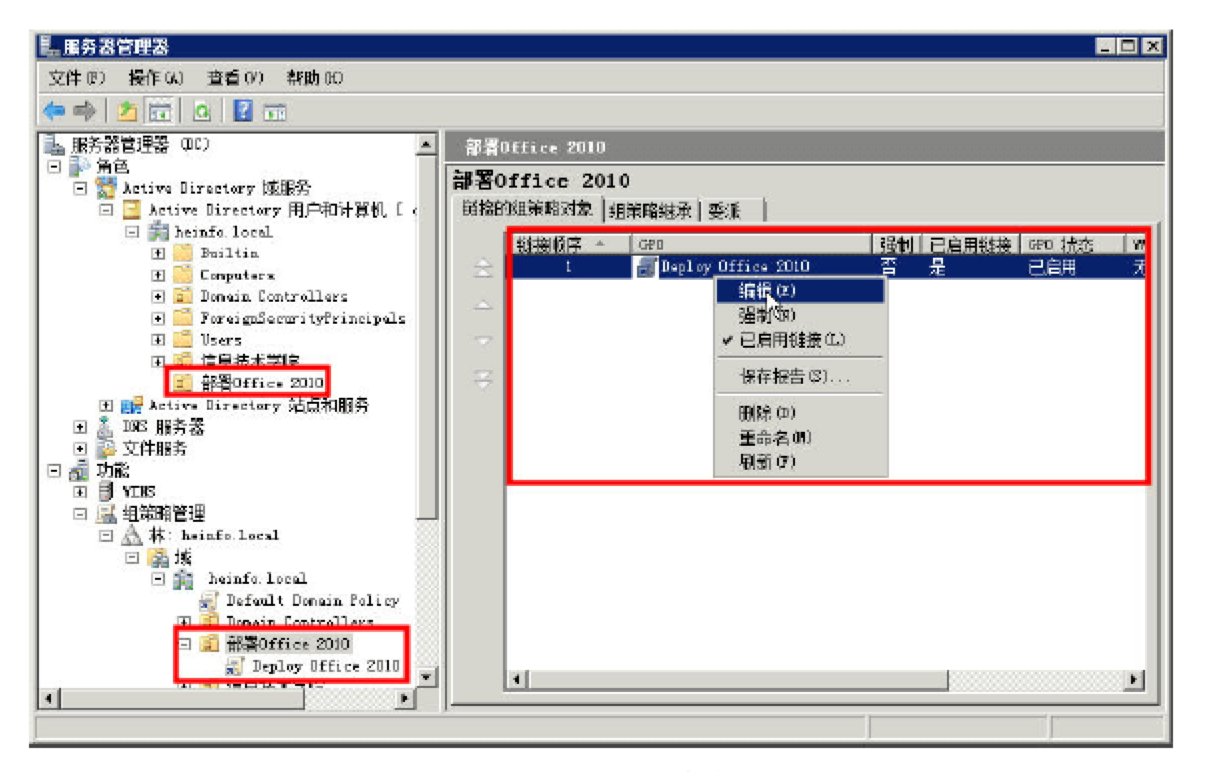


图 8-146 创建并编辑组策略

03 打开“组策略管理编辑器”窗口，定位到“计算机配置→策略按钮→Windows 设置→脚本（启动/关机）”，用鼠标右击右侧的“启动”选项，在弹出的快捷菜单中选择“属性”选项，如图 8-147 所示。

04 打开“启动 属性”对话框，单击“显示文件”按钮，如图 8-148 所示。

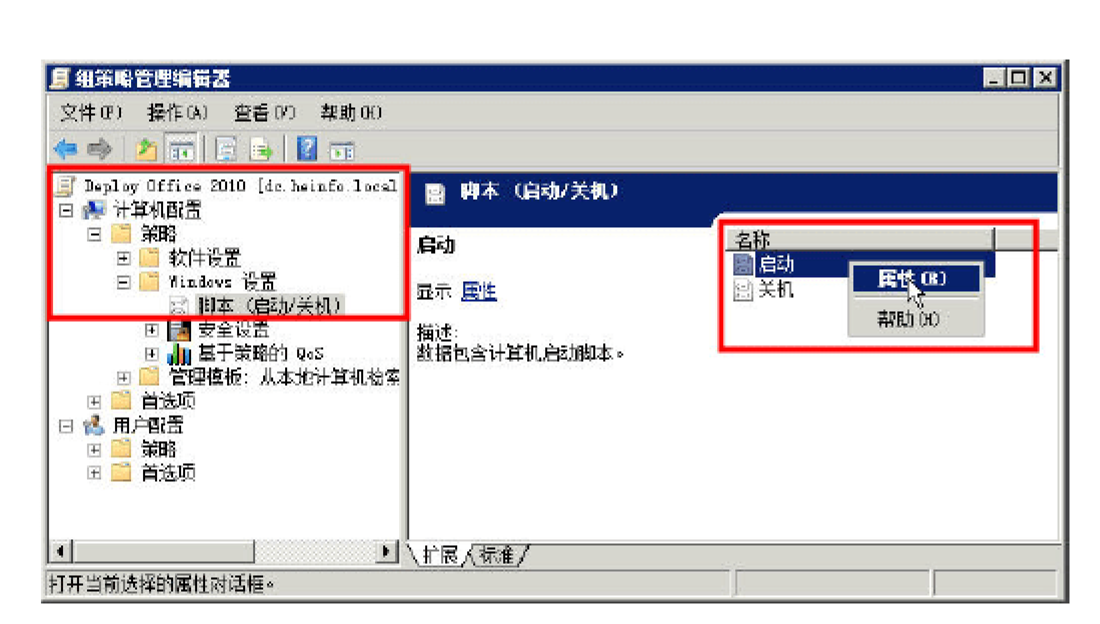


图 8-147 启动脚本

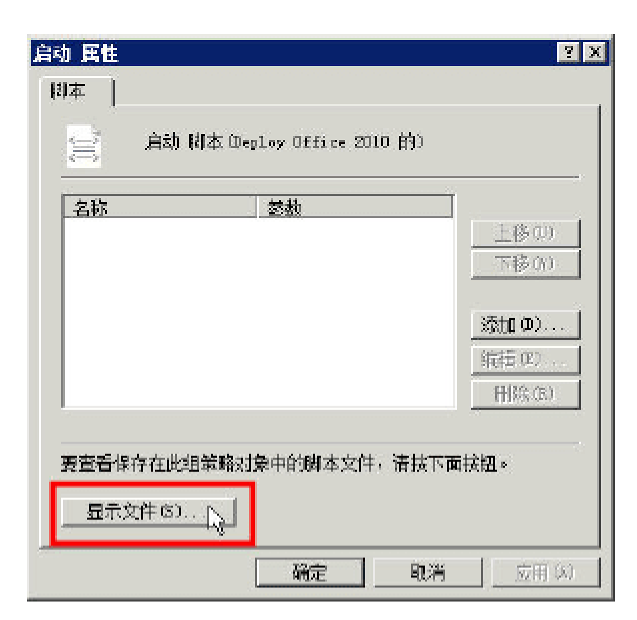
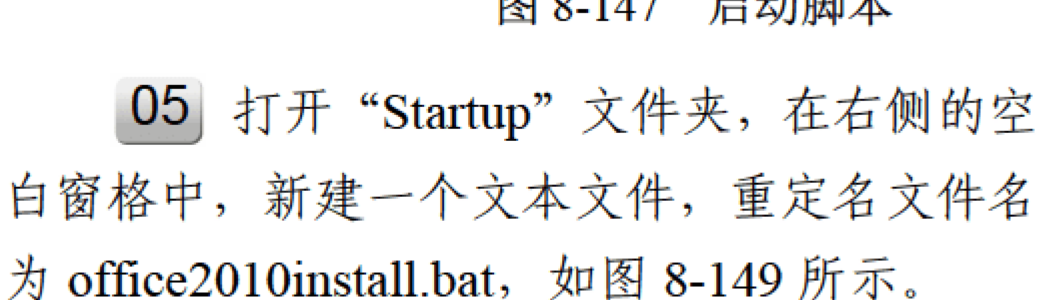


图 8-148 显示文件



05 打开“Startup”文件夹，在右侧的空白窗格中，新建一个文本文件，重定名文件名为 office2010install.bat，如图 8-149 所示。

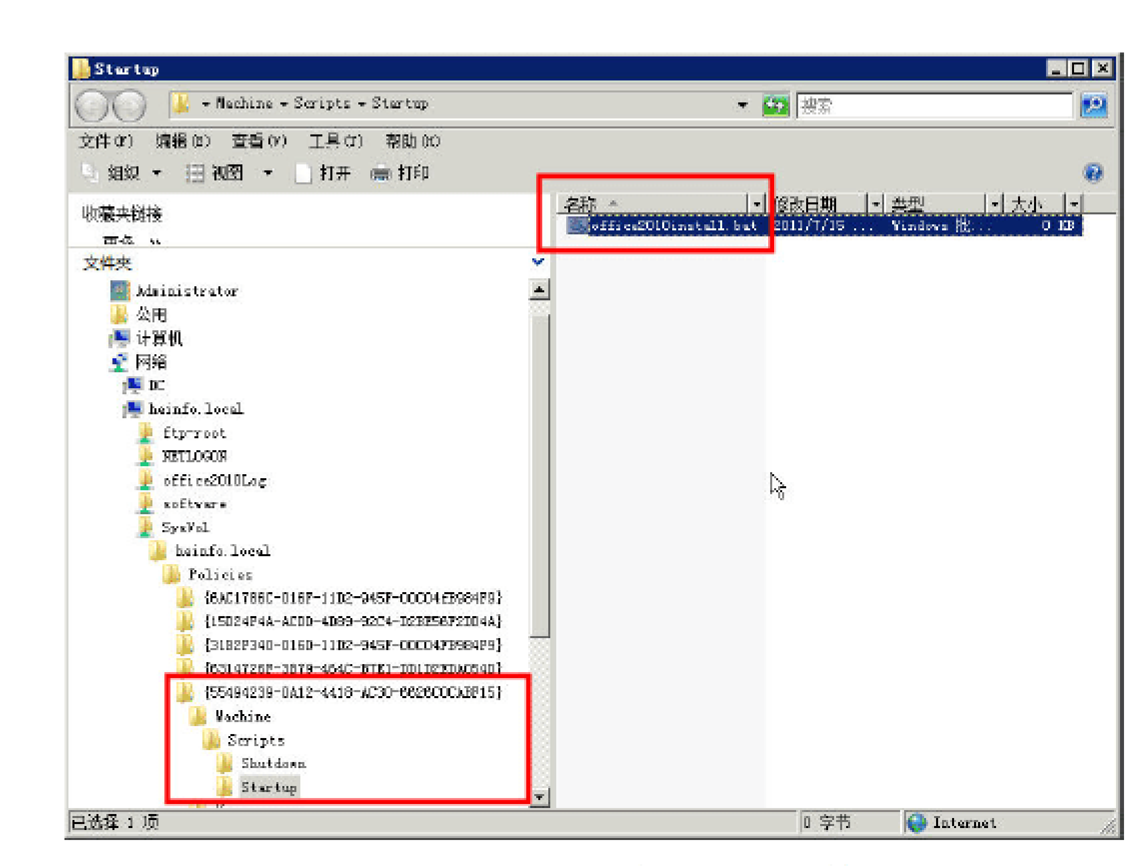


图 8-149 新建批处理文件

06 用“记事本”打开 office2010install.bat 之后，编写 Office 2010 的自定义安装脚本，脚本的关键是能实现“全自动”运行 Office 2010 的安装程序并能在无人交互的方式下，完成 Office 2010 的安装。要实现这些功能，用户可以使用 8.6.2 或 8.6.3 两节中的任意一种方式，例如，如果要使用自定义配置文件安装 Office 2010，则安装命令是：

```
setup /adminfile updates\office2010pro.msp
```

如果要使用配置文件，则安装命令是：

```
setup.exe    /config    proplus.ww\config.xml
```

当然，在实际的使用中，由于安装程序是保存在服务器上的，所以，无论是安装程序，还是配置文件或自定义文件，都要使用 UNC 路径。另外，由于 Office 2010 有 32 位版本与 64 位版本，而操作系统亦有 32 位与 64 位之分，32 位的 Office 2010 可以安装在 32 位与 64 位的操作系统上，而 64 位的 Office 2010，只能安装在 64 位的操作系统上，在编写脚本的时候，也需要考虑这个问题。下面的脚本，将以分发 Office 2010 的 32 位版本为例，自动识别 32 位与 64 位操作系统，并启动 Office 2010 的安装过程。脚本内容如下（本方法使用自定义配置文件）：

```
setlocal

REM ***********************************************************************
REM Environment customization begins here. Modify variables below.
REM ***********************************************************************

REM  设置 Office 2010 的产品名称，在安装完成之后，将会在注册表中使用此名称注册键值.
set ProductName=Office14.PROPLUS

REM  设置 Office 2010 安装文件路径，注意，需要使用 UNC 网络路径.
set DeployServer=\\dc\software\Office2010

REM  设置 Office 2010 配置文件及路径
set ConfigFile=\\dc\software\Office2010\ProPlus.WW\config.xml

REM  设置 Office 2010 自定义文件及路径
set CustomFile=\\dc\software\office2010\updates\office2010pro.msp

REM  设置 Office 2010 安装日志路径，该路径必须有可写权限
set LogLocation=\\dc\office2010Log

REM ***********************************************************************
REM  下面为部署 Office 2010 的代码，一般不用修改.
REM ***********************************************************************

REM  检查 64 位操作系统中存在的变量，32 位操作系统不存在该变量
REM  如果%ProgramFiles（x86）%变量存在，当前系统是 64 位，不存在则是 32 位
IF NOT "%ProgramFiles（x86）%"=="" （goto ARP64）else（goto ARP86）

REM  操作系统是  X64. 检查 32 位 Office 2010 的反安装键值  Wow6432 是否存在
:ARP64
REM  查询注册表键值，如果存在返回 0，如果不存在，返回 1
reg query HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Microsoft\Windows\CurrentVersion\Uninstall\%ProductName%
REM  如果返回值不等于 1 则结束（键值不存在则继续）
if NOT %errorlevel%==1 （goto End）

REM  检查 32 位与 64 位系统中 Office 2010uninstall key 是否存在
:ARP86
```

```
reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\%ProductName%
REM 如果不存在，返回 1，则开始部署 Office ，如果存在则结束
if %errorlevel%==1（goto DeployOffice）else（goto End）

REM 如是返回值是 1，表示 Office 2010 不存在，运行安装程序
:DeployOffice

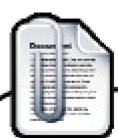
REM 使用配置文件 config.xml 开始安装
REM start /wait %DeployServer%\setup.exe /config %ConfigFile%

REM 使用自定义文件开始安装
REM start /wait %DeployServer%\setup.exe /adminfile %CustomFile%

REM  安装结果输出到 Office 2010 安装日志
echo %date% %time% Setup ended with error code %errorlevel%. >> %LogLocation%\%computername%.txt

REM If 0 or other was returned, the product was found or another error occurred. Do nothing.
:End

Endlocal
```



说 明

在该脚本文件中，有四个变量：

第 1 个变量为\\dc.heinfo.local\software\Office2010，表示 Office 2010 安装程序所在路径。

第 2 变量个为\\dc.heinfo.local\software\Office2010\ProPlusr.WW\，表示 config.xml 文件及路径。

第 3 变量个为\\dc\software\office2010\updates\office2010pro.msp，表示自定义文件及路径。

第 4 个变量为“\\dc.heinfo.local\office2010Log”，表示安装 Office 2010 的日志文件。

如果是在自己的网络中，须用自己的服务器的计算机名称与共享名称替换以上文件。该脚本文件也可以从 http://technet.microsoft.com/zh-cn/library/ff602181.aspx 下载之后，并参考本书修改。

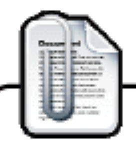
如果要使用配置文件进行安装，须将

```
REM start /wait %DeployServer%\setup.exe /config %ConfigFile%
```

一行中前面的 REM 去掉，并在

```
start /wait %DeployServer%\setup.exe /adminfile %CostomFile%
```

一行最前面加入 REM 及一个空格进行分隔。



注 意

不同版本 config.xml 保存的路径不同，在 Office 2010 的 VL 版本中，保存路径是 ProPlus.WW，其他版本是 ProPlusr.WW。

07 编写脚本并保存后，返回到“启动 属性”对话框，单击“添加”按钮，在弹出的“添加脚本”对话框中，单击“浏览”按钮，选择图 8-149 中创建的文件 office2010install.bat，如图 8-150

所示，然后两次单击“确定”按钮返回。

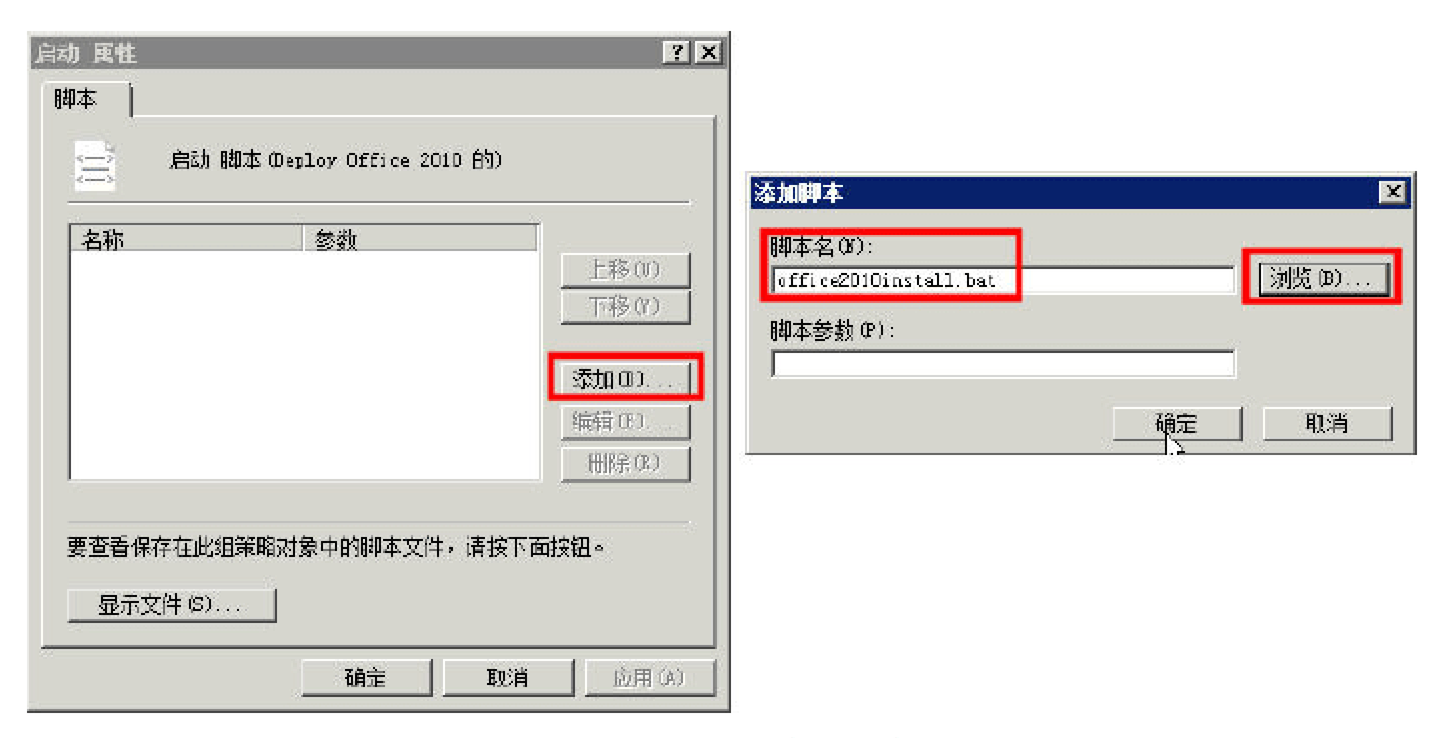


图 8-150 添加脚本

08 定位到“计算机配置→策略→管理模板→系统→脚本”，双击右侧的“组策略脚本的最长等待时间”选项，在“设置”选项卡中，将其修改为 0，表示让系统一直等到脚本完成运行（默认是 600s），如图 8-151 所示。

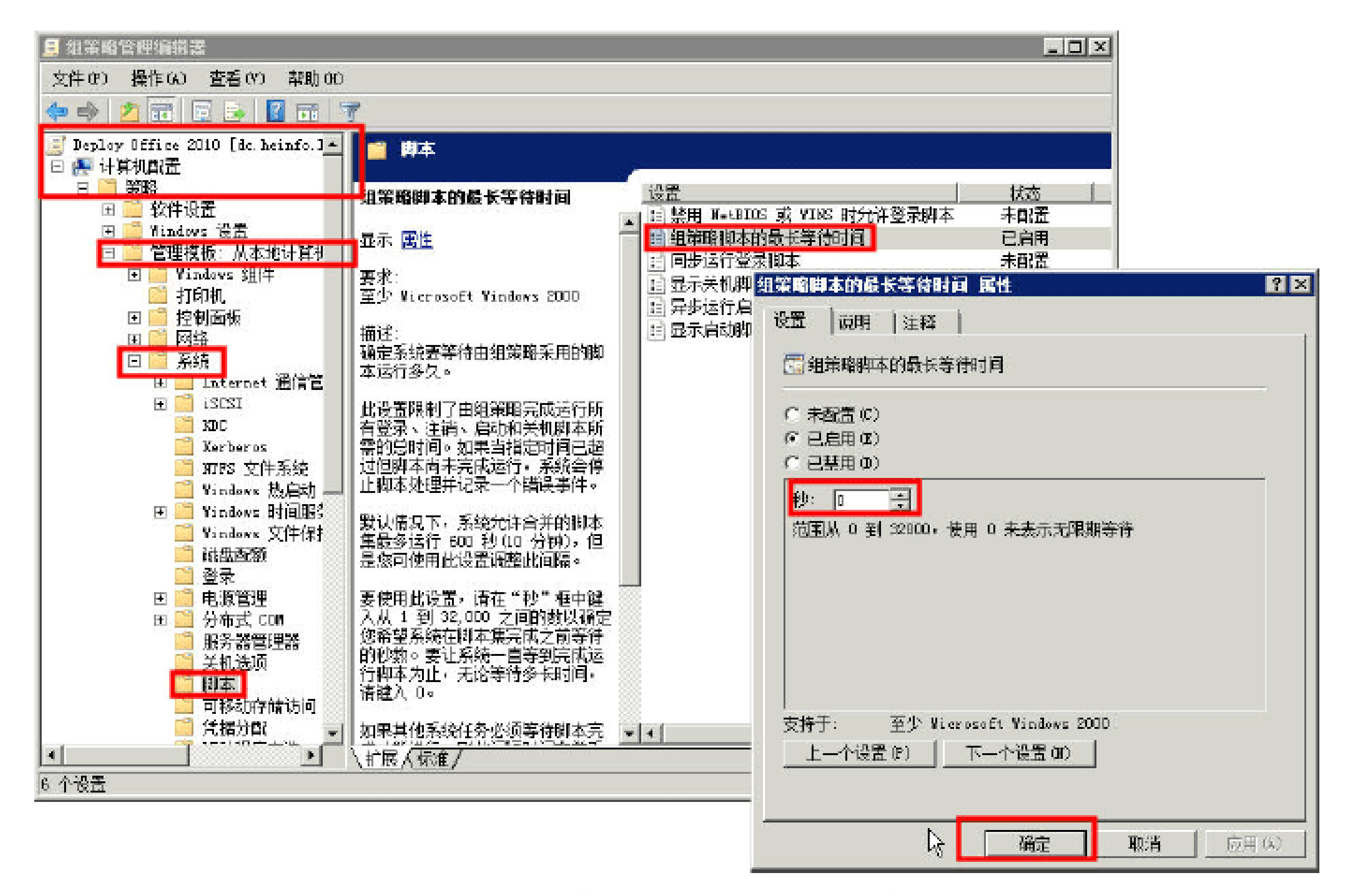


图 8-151 修改脚本最长等待时间

8.6.5 使用组策略自定义 Office 2010

8.6.4 小节的组策略及脚本是实现在“计算机”中安装 Office 2010 的功能。如果要为用户自定义 Office 2010 的环境，可以在“用户配置”中，通过添加 Office 2010 组策略模板实现，主要步骤如下。

01 打开“信息技术学院”组策略管理编辑器，定位到“用户配置→策略→管理模板”，用鼠标右击，在弹出的快捷菜单中选择“添加/删除模板”选项，如图 8-152 所示。

02 在弹出的“添加/删除模板”对话框中，单击“添加”按钮，然后浏览选择图 8-128 中 Office 2010 自定义工具的解压缩目录，从 adm\zh-cn 中选择并添加 office14.adm，如图 8-153 所示。添加之后，返回到“添加/删除模板”对话框，单击“关闭”按钮，完成添加。

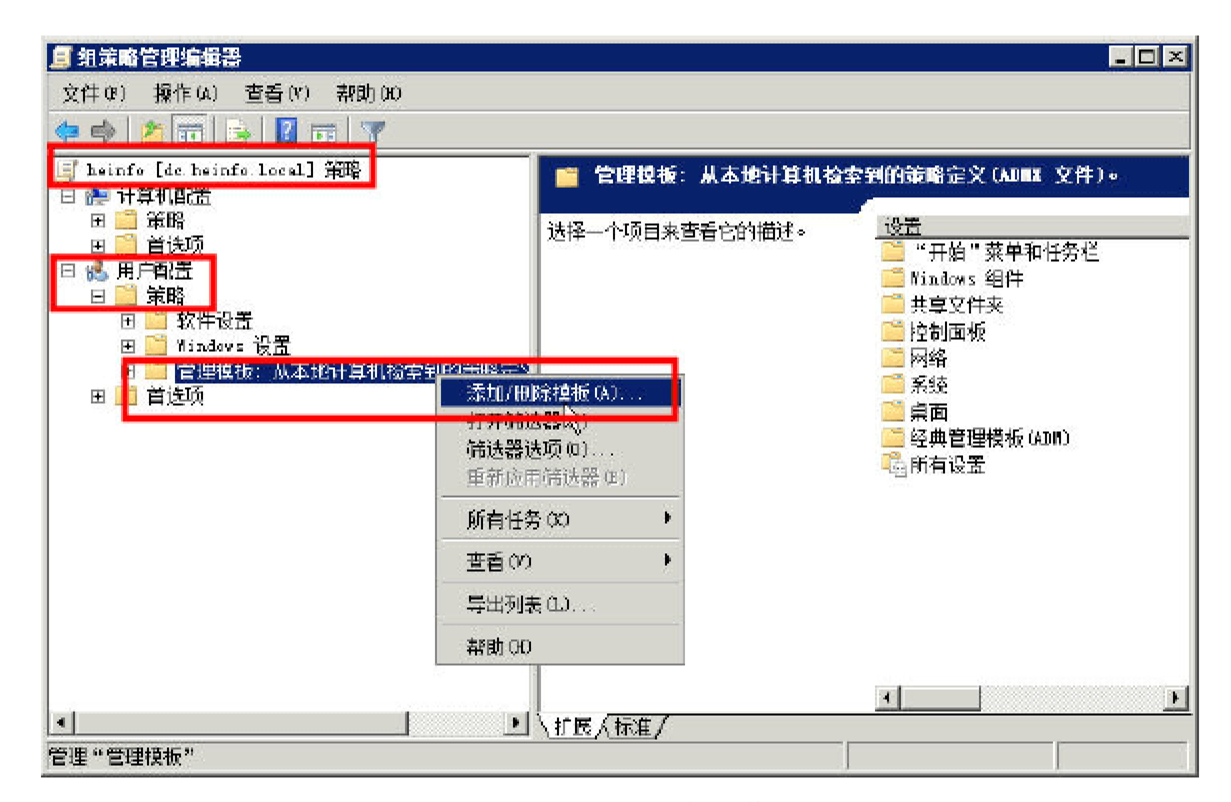


图 8-152　添加模板

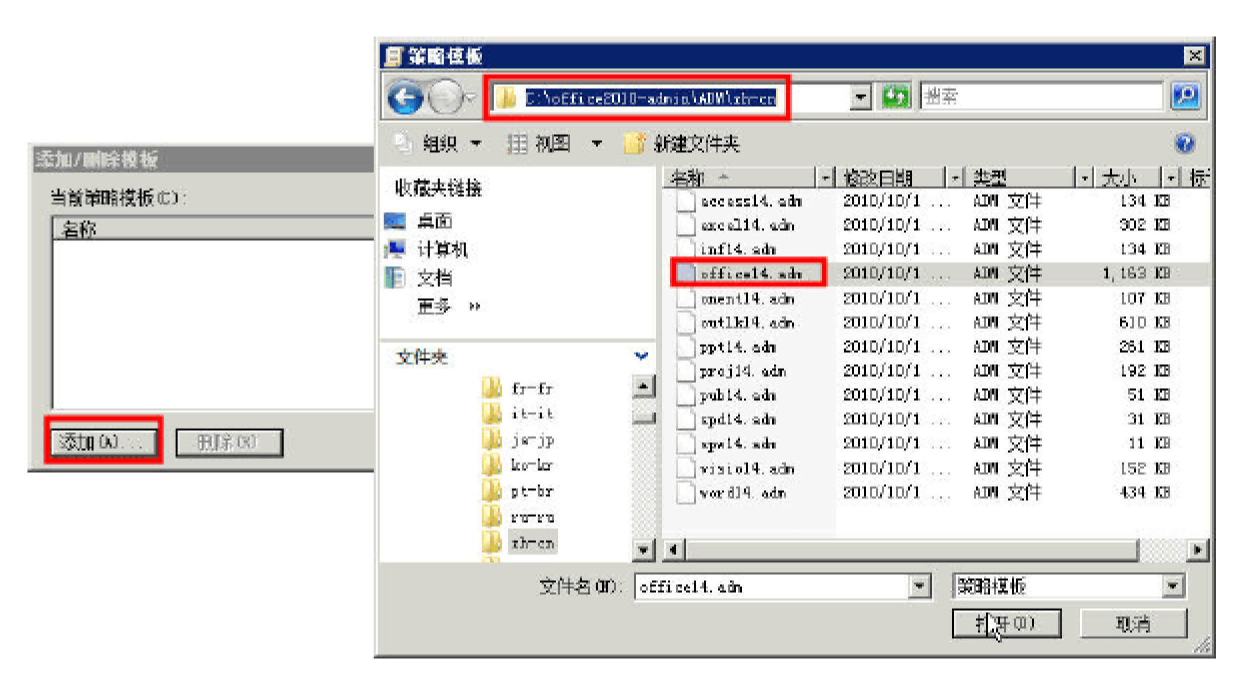


图 8-153　添加 office14 策略模板

03 然后定位到“用户配置→策略→管理模板→经典管理模板→Microsoft Office 2010”策略组，就可以对 Office 2010 进行定义了，如图 8-154 所示。

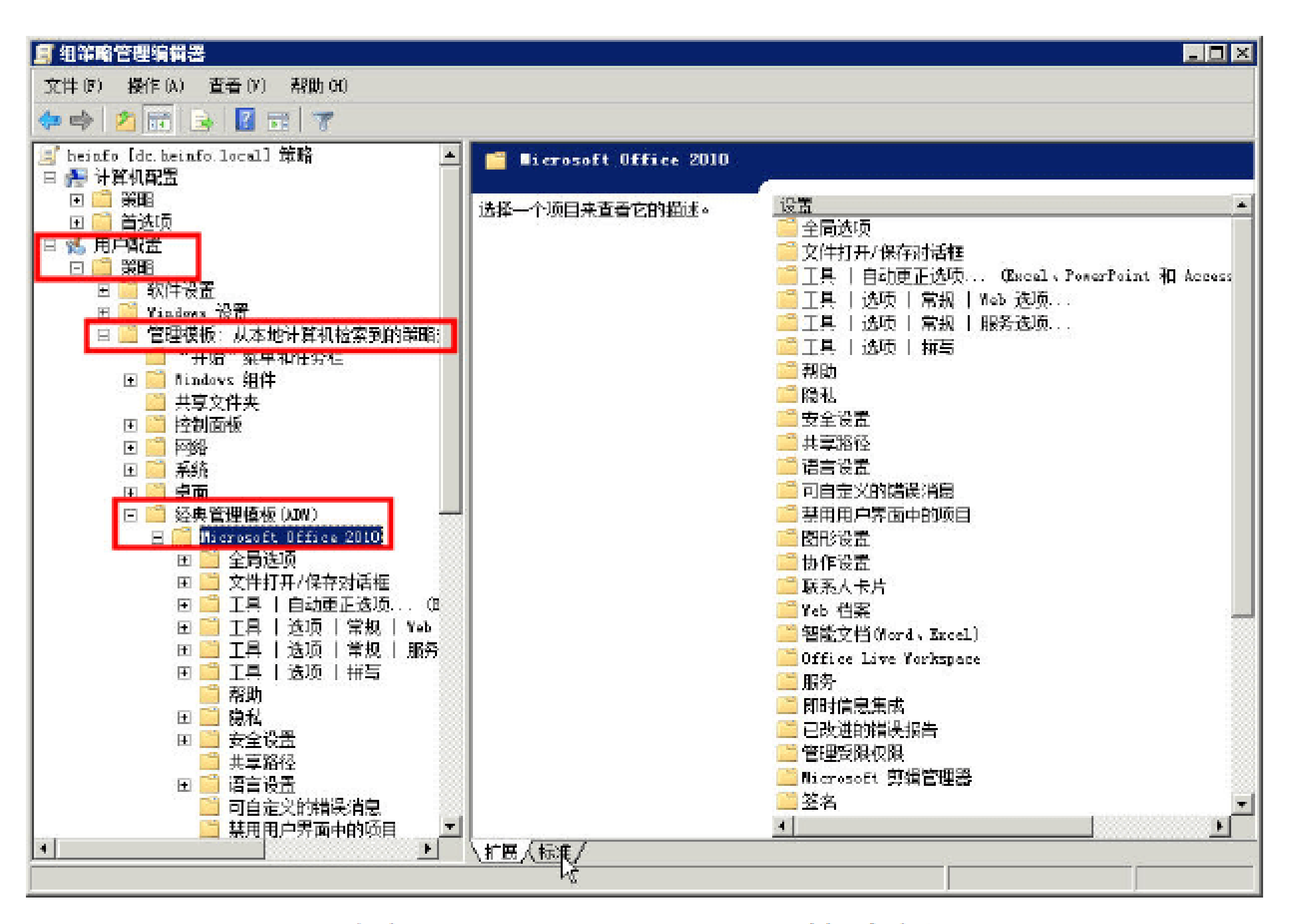


图 8-154　Office 2010 策略组

04 最后在命令提示符中执行 gpupdte /force，刷新组策略。

8.6.6　在 Windows 7 客户端测试

本小节就可以在 Windows 7 客户端测试 Office 2010 的分发了，主要步骤如下。

01 在“服务器管理器”窗口中，将要安装 Office 2010 的计算机移动到“部署 Office 2010”组织单位中，如图 8-155 所示。

02 以域管理员账户 heinfo\administrator，如图 8-156 所示。

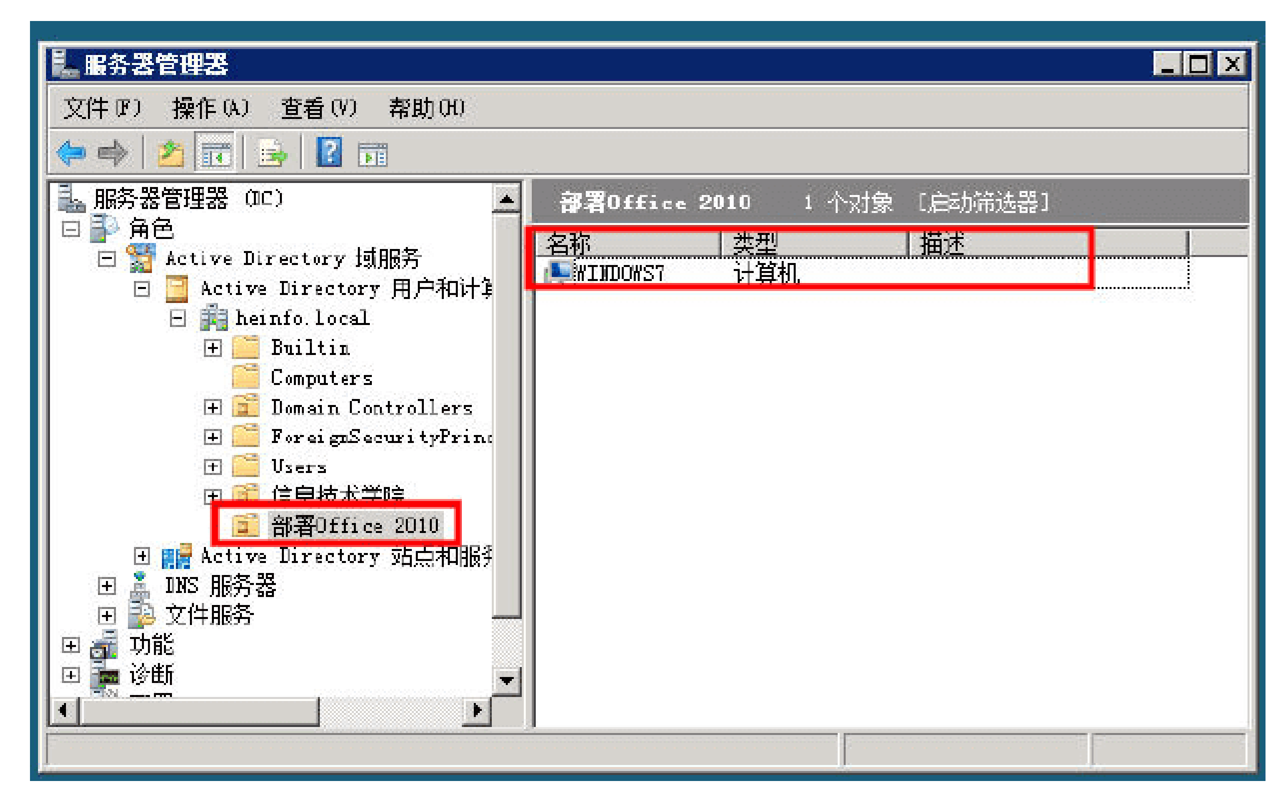


图 8-155 移动 Windows7 计算机到组织单位中



图 8-156 以域管理员账户登录

03 随后会进入系统，此时，不会看到 Office 2010 的安装界面，安装程序会在后台运行，可以通过“Windows 任务管理器”，在“联网”选项卡中看到网络使用率比较高（如图 8-157 所示），在“进程”选项卡中还会看到 setup.exe 的进程。

04 用户可以切换到 Windows 2008 的服务器中，打开“计算机管理”窗口，在“系统工具→共享文件夹→打开文件”中，看到以“Windows7$”的计算机名称打开并访问的 E:\software\Office2010 的安装文件，如图 8-158 所示。

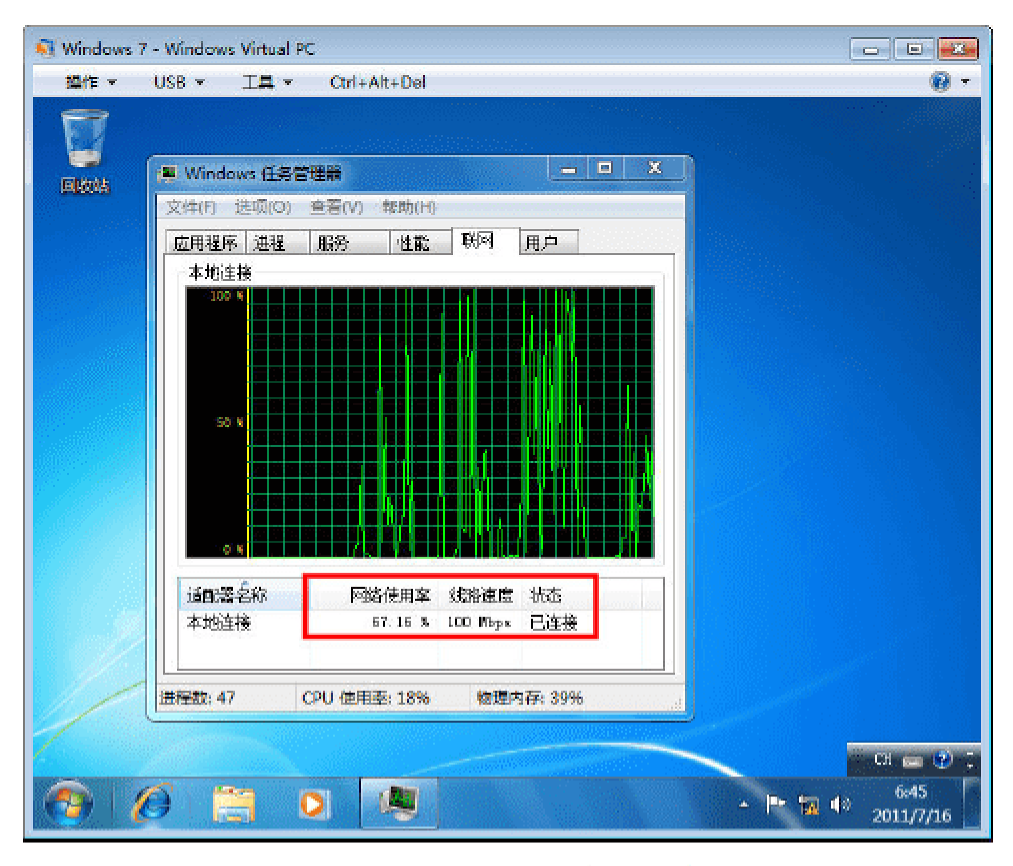


图 8-157 网络使用率

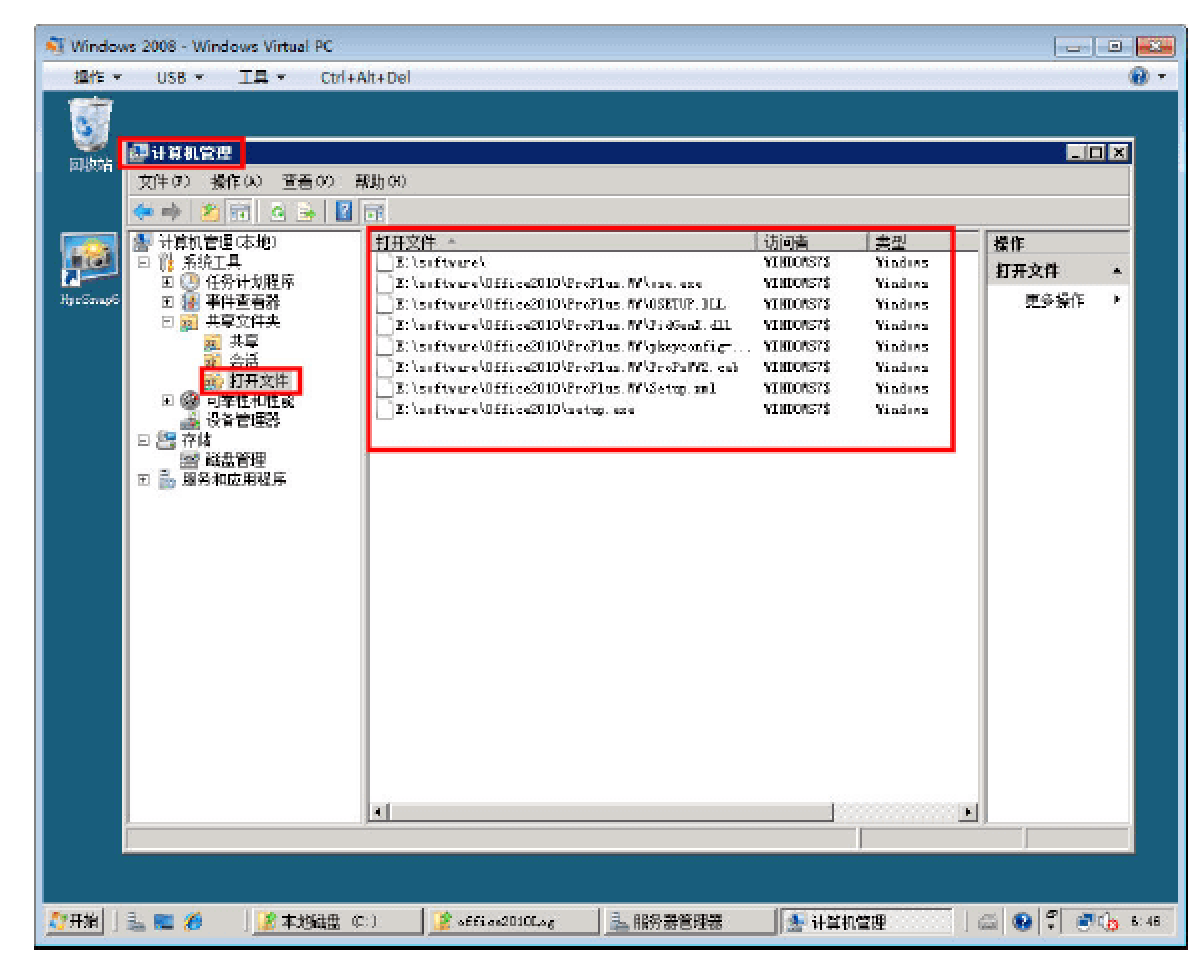
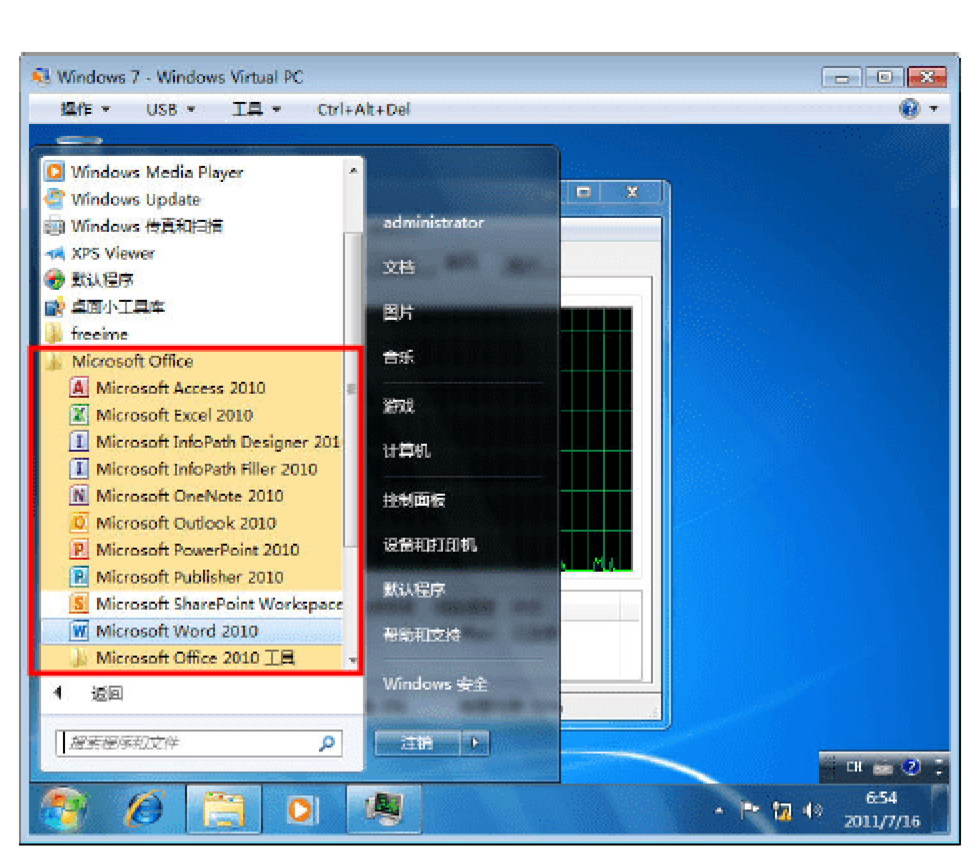


图 8-158 在服务器查看共享文件夹的使用情况

05 等过一段时间之后，在 Windows 7 的工作站端，从“开始菜单→所有程序”中会看到“Microsoft Office”的程序文件夹，表示 Office 2010 部署完成，如图 8-159 所示。

06 用户也可以查看 Office 2010 日志文件夹，在此显示了安装结果（每个文件名代表部署了一个计算机，并以计算机名称为文件名），如图 8-160 所示。



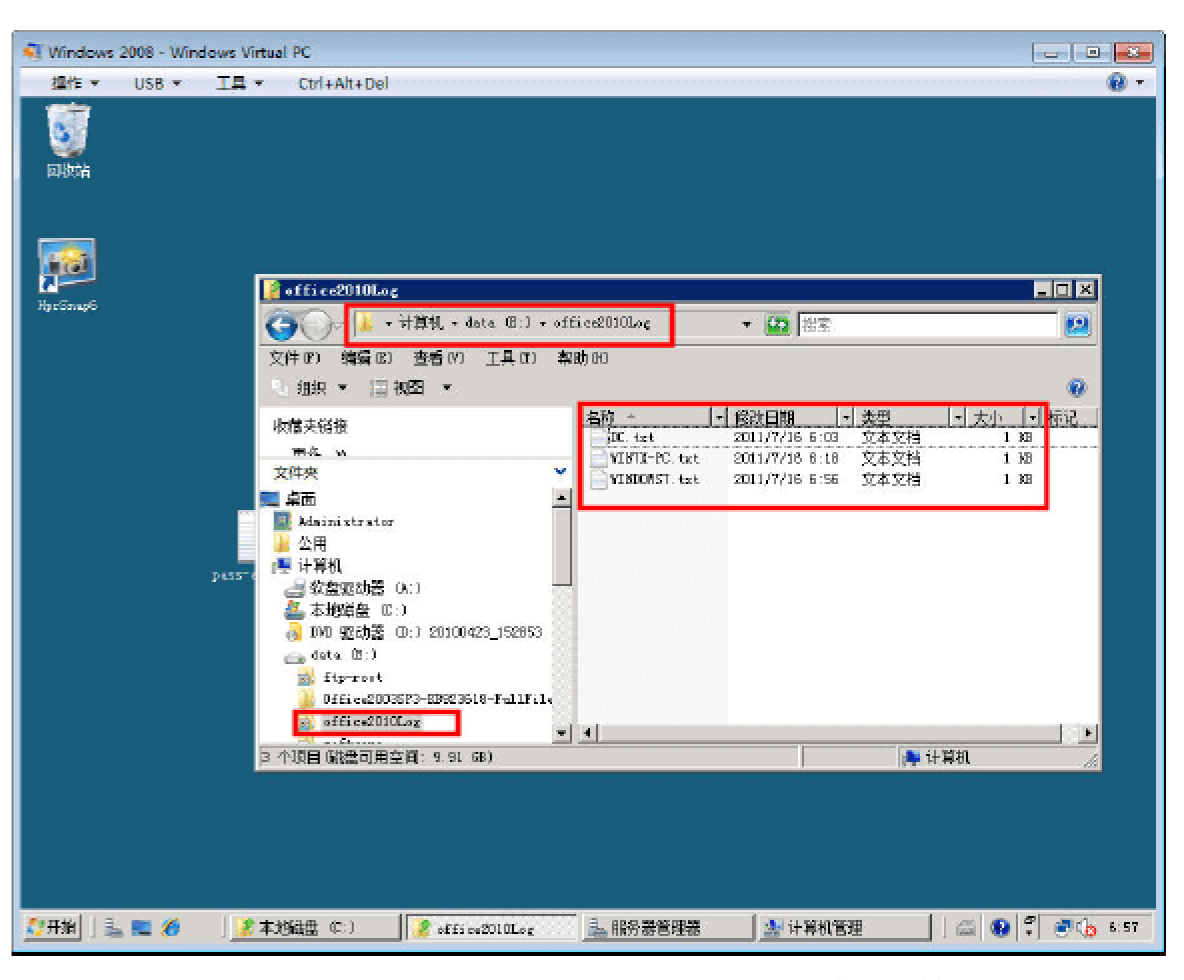



图 8-159　Office 2010 部署完成

图 8-160　Office 2010 日志文件

07 打开可以查看部署的结果，如果文件内容中有日期及代码 0，表示部署成功；如果代码不为 0，则表示部署出现问题，如图 8-161 所示。

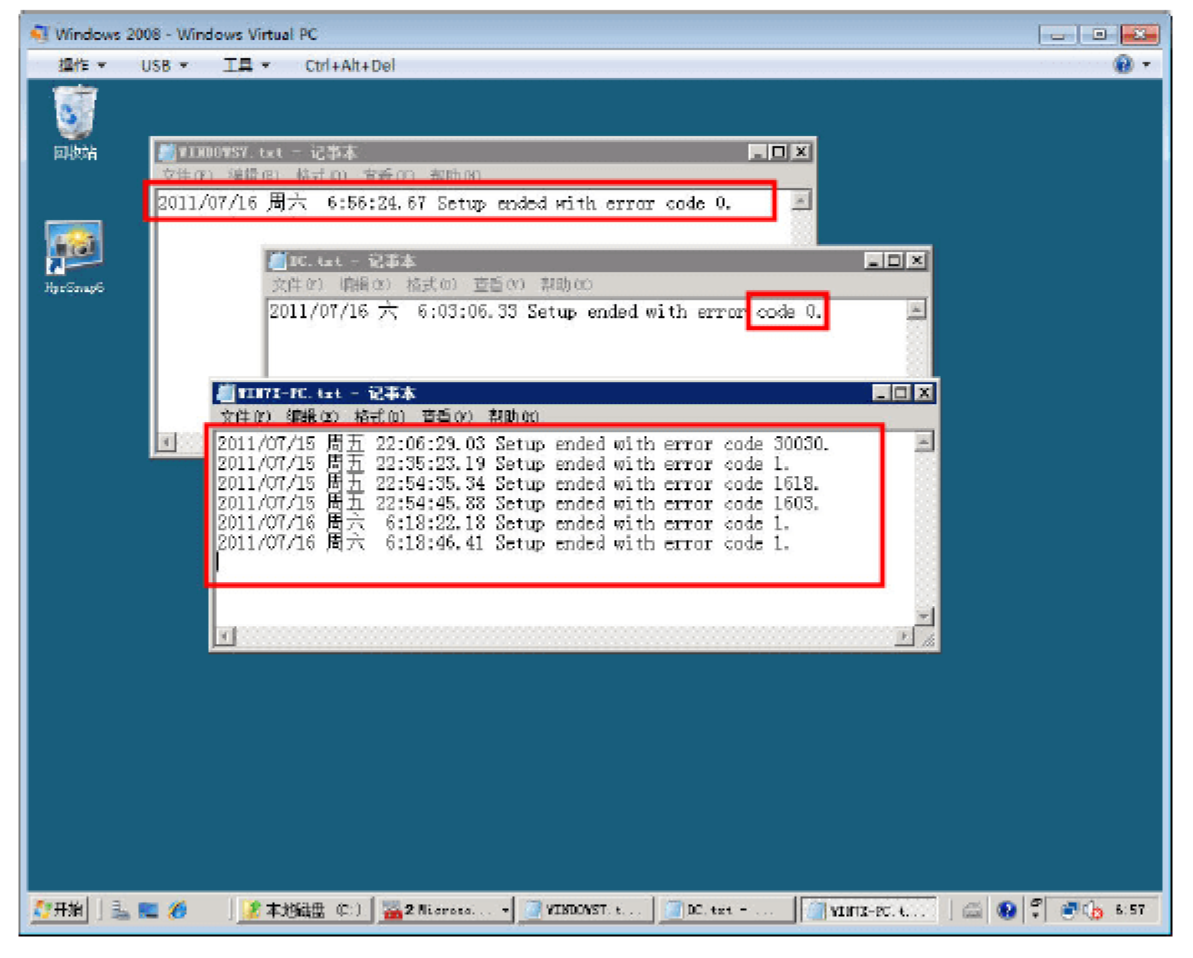


图 8-161　部署结果

说 明

日志文件中的返回代码 0 表示安装成功完成。返回代码 3010 表示需要重新启动。有关 Office 产品的 Windows Installer 进程的其他错误代码的详细信息，请参阅 Microsoft 知识库文章 290158：Office 2003 产品和 Office XP 产品中 Windows Installer 进程的错误代码和错误信息列表，该产品链接主页为 http://support.microsoft.com/kb/290158/zh-cn。

8.7　组策略的应用效果

在本节，我们来查看使用组策略的应用效果。以 Windows XP 工作站、用户 ws01 为例（将

ws01 用户移动到“信息技术学院”组织单位中）进行介绍。

8.7.1 以域用户的身份登录到工作站

如果要使组策略的设置能够应用于用户，在已经加入域的工作站上，必须以域用户的身份登录，否则组策略应用没有任何效果，如图 8-162 所示。



图 8-162 以域用户 ws01 登录

8.7.2 自动添加的程序

在工作站上以域用户登录后，经过组策略定制的环境、分发的软件就会开始生效。如果是“指派”的软件，在第一次使用时将会自动进行安装。

01 打开“开始”菜单，在所有“程序”菜单中显示的是根据组策略部署的软件，例如前面使用组策略指派的 Office 2003，如图 8-163 所示。

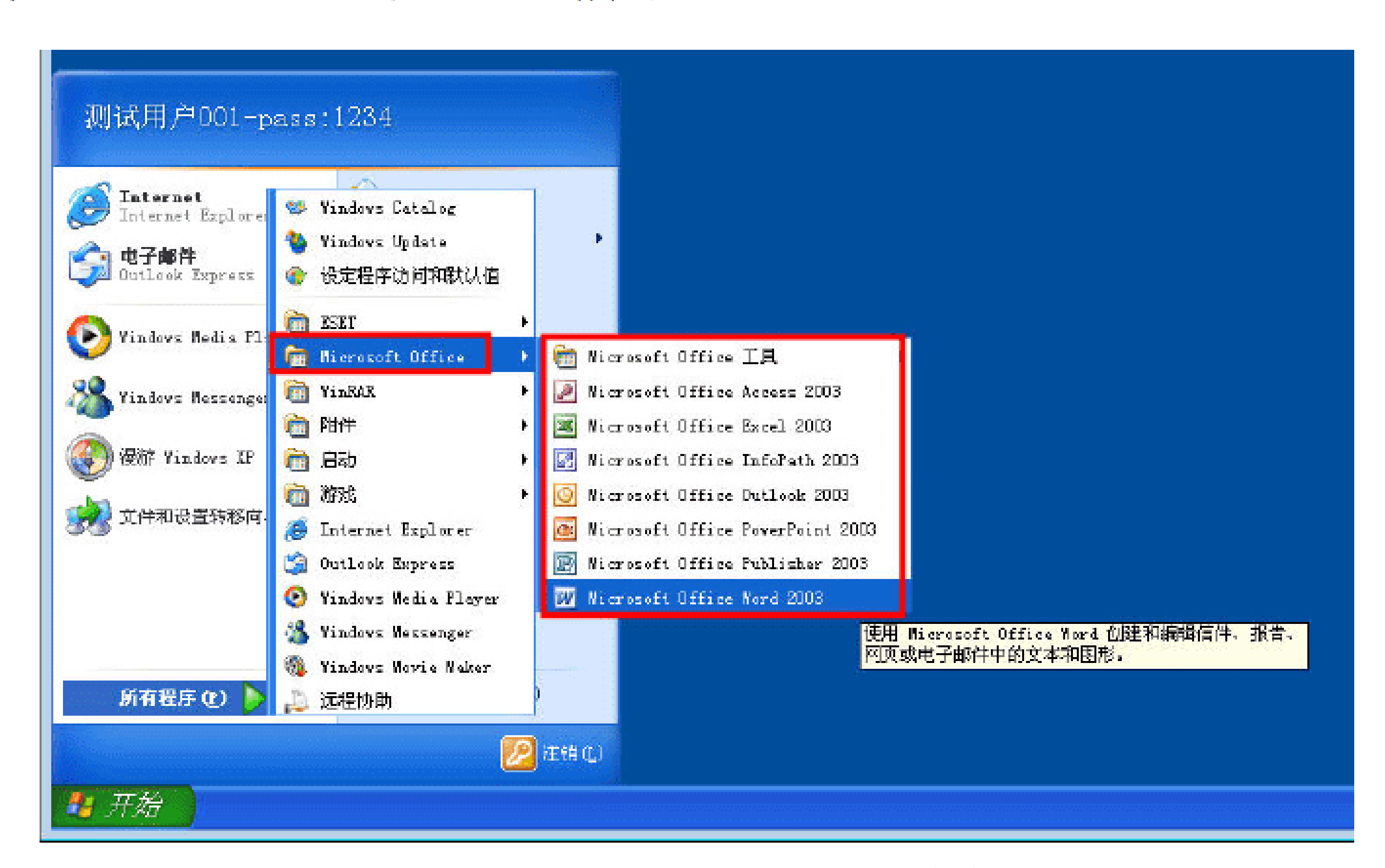


图 8-163 Office 2003 已经安装

02 需要注意的是，这些只是应用软件的快捷方式，而应用软件还没有安装。在第一次使用的时候，这些软件会自动安装，如图 8-164 所示。

03 等待几分钟，安装完成后就会进入 Word 界面了。以后再次运行 Word 时将会直接进入，不需要再次安装。

Microsoft Office Professional Edition 2003

Windows 正在设置 Microsoft Office Professional Edition 2003，请稍候。

取消

图 8-164　第一次使用时开始安装

8.7.3　手动添加的程序

从“控制面板”中打开“添加或删除程序”窗口，选择“添加新程序”选项，所有已经“发布”的软件将显示在此处，如图 8-165 所示。



图 8-165　管理员发布的软件

单击要添加的程序，开始软件的安装，如图 8-166 所示。按照正常的安装步骤，安装软件即可。



图 8-166　安装已经发布的软件

8.7.4　查看组策略定制的环境

打开 IE 浏览器，可以看到经过组策略定制的 IE 首页，如图 8-167 所示。由于当前所用虚拟机的设置，当前计算机并不能打开所设置的主页。

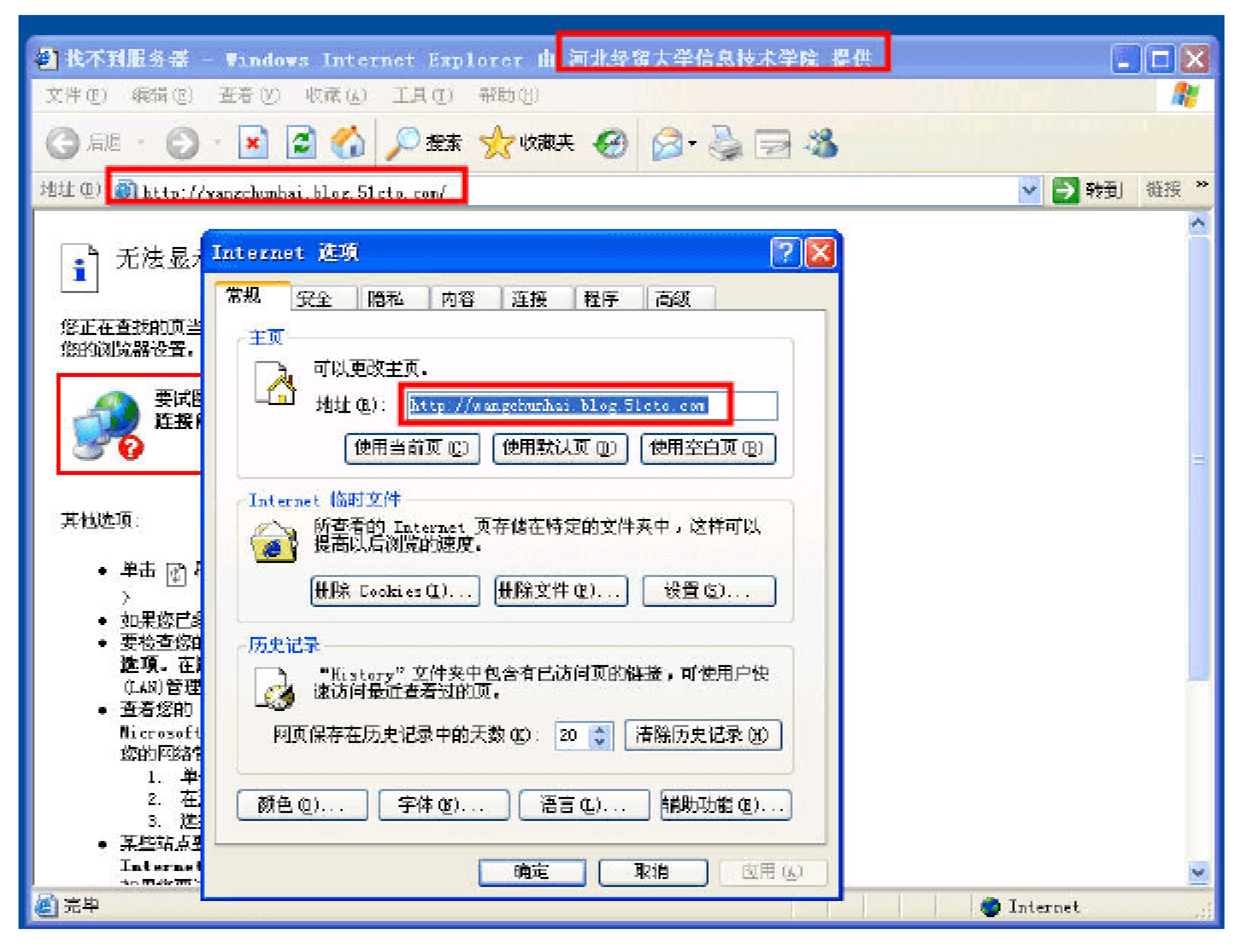


图 8-167　IE 设置

如果在打开 IE、我的文档时，出现“打开文件-安全警告”的提示框（如图 8-168 所示），单击“打开”按钮即可。

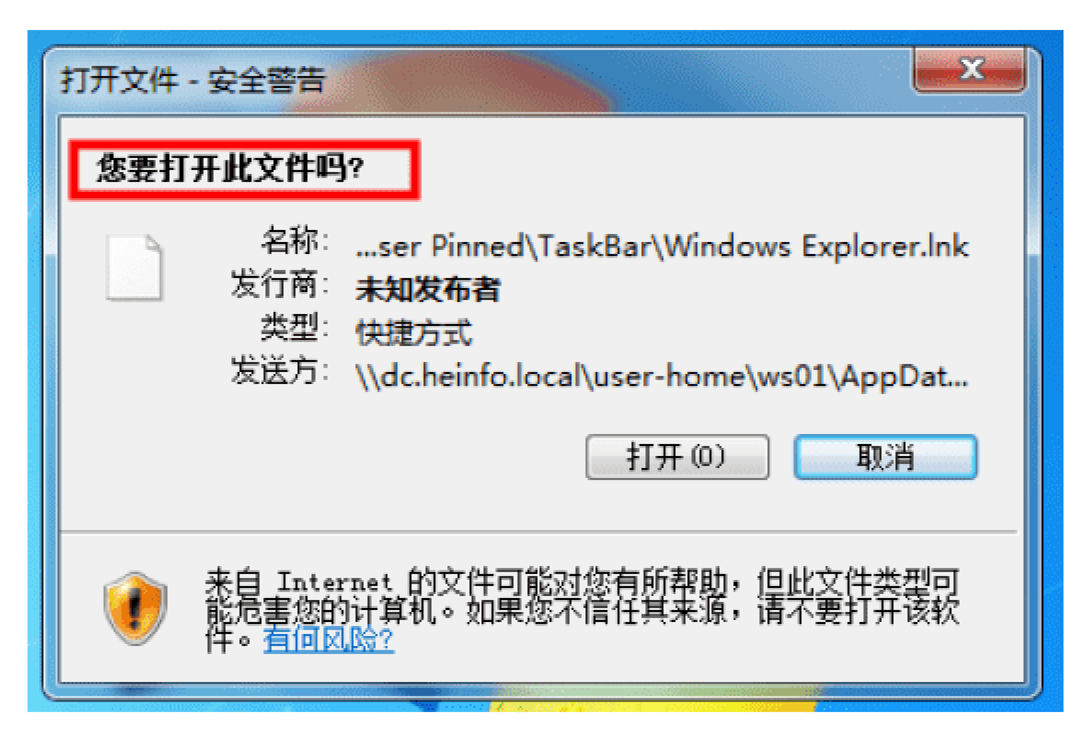


图 8-168　打开文件警告对话框

第 9 章　使用 RMS 保护企业内部的 Office 文档

文件安全是网络领域中最重要的课题之一。许多企业的规章制度、机密资料已经电子化，而这些文档大部分又是 word 文档。企业中的员工只要能读取并打开这些文档，就可以将这些重要资料复制、打印。如何在不影响员工查阅的情况下又能确保这些资料的安全呢？使用 Microsoft 的 Rights Management Services（RMS，权限管理服务）即可解决这个问题。RMS 通过数字证书和用户身份验证技术对各种 Office 文档的访问权限加以限制，使用户只能查看文档内容，而不能打印和复制，可以有效防止内部用户擅自泄漏机密文档内容，从而确保了数据文件访问的安全性。

9.1　RMS 概述

RMS（权限管理服务）能够有效的保护文档在相应授权范围之内不会泄露。在 Windows Server 2008 中为 AD RMS（Active Directory Rights Management Services），即活动目录权限管理服务。相对于 Windows Server 2003 下的 RMS 有了较大的改进与提升，通过和 Active Directory 联合身份验证等服务的配合使用，可以更好地保护 Office 文档的权限，而且使应用更加方便。

9.1.1　AD RMS 的相关组件

AD RMS 仍然基于服务器/客户端的结构，其主要组件包括支持 AD RMS 的应用程序、AD RMS 客户端和 AD RMS 服务器端 3 项，三者缺一不可。只有支持 AD RMS 的应用程序才能生成被保护的文档；AD RMS 客户端是安装在客户机上的，与支持 AD RMS 的应用程序进行交互；AD RMS 服务器负责为信任实体颁发证书、授权服务器、为 AD RMS 保护的文档进行授权。

使用权限管理账户证书可以将用户账户和具体的一台设备关联起来，也就是说每个不同的账户在同一台计算机上存在惟一的权限管理证书，或同一账户在不同的计算机上的权限管理证书也不相同。虽然在不同计算机上的权限管理账户证书不同，但是在权限管理账户证书中所包含的密钥却是相同的。该权限管理账户证书是由企业中的第一台 AD RMS 服务器所颁发的，即在任何计算机上的用户的密钥对是相同的，当用户向 AD RMS 许可服务器请求许可时就需要使用权限管理账户证书。

权限账户证书（RAC）的生成过程如下所示。

（1）当用户第一次使用由 AD RMS 加密的文档时，就需要向 AD RMS 服务器发送请求，首先用户会以域用户的身份向 AD RMS 证书服务器发送请求，来获取权限管理账户证书。

（2）服务器会对服务器数据库中所存的信息进行查询，如果该用户已经存在密钥对，就会应用已有的密钥；如果没有，就会为该用户生成一个密钥对。

（3）服务器会将该用户的密钥对中的私钥用该证书服务器的私钥进行加密。

（4）将用户密钥对中的私钥加密后，服务器会将用户密钥对中的公钥和加密后的私钥放到权限管理账户证书中。

（5）权限管理账户证书会被 AD RMS 服务器用私钥进行数字签署，这样就能确定该权限管理账户证书是由 AD RMS 证书服务器所发放的，还没有被篡改。

（6）AD RMS 服务器会将权限管理账户证书发送给用户。

（7）服务器将用户的密钥对存储到 AD RMS 的数据库中，该权限管理账户证书就是以后该用户进行各种使用许可申请的证书。

9.1.2　AD RMS 的实现原理

1. 服务的发现

服务的发现实际上就是 RMS 客户端发现 AD RMS 服务器的一个过程，该过程可以通过两种方法来实现，一种是通过活动目录中的服务连接点（SCP），通过它就可以找到企业中的证书服务器的位置。第二种方法就是通过注册表，通过注册表可以使客户端上的应用程序找到 AD RMS 服务器。

AD RMS 服务可以激活 RMS 客户机，如果要使用该 RMS 客户机，必须在第一次使用时去 AD RMS 服务器上激活该 RMS 客户机，因为这样就可以从 AD RMS 服务器上获取权限管理账户证书等信息。

2. 文档的在线发布过程

由 RMS 客户端在线向授权服务器发送请求。具体的发布过程如下。

（1）由密码箱生成对称密钥作为内容密钥，这个内容密钥会被授权服务器加密。

（2）内容密钥会被授权服务器的公钥加密，这样做的目的就是通过网络将它发送给授权服务器，然后授权服务器能够用它自己的私钥将这个内容解读出来，而在传送的过程中不会被别人截获获取内容密钥。

（3）加密的内容密钥和权限被发送给请求发布许可的授权服务器。

（4）授权服务器使用它的私钥解开加密的内容密钥。

（5）授权服务器使用它的公钥加密内容密钥和使用权限。

（6）加密后的密钥和使用权限被添加到发布许可。

（7）授权服务器使用它的私钥签署发布许可。

（8）发布许可返回给申请的客户端。

（9）支持 AD RMS 的应用程序将发布许可合并到受保护的文档中。

3. 文档的离线发布过程

如果用户使用的是笔记本等移动办公的计算机设备，在自己的家中有可能不能够连接到公司的 AD RMS 服务器，这时该用户是不是就不能使用由 AD RMS 创建的文档了呢？其实用户还是可以访问这些文档的，只是用户需要一个客户端许可证书（CLC）。具体的保护过程如下。

（1）由密码箱生成对称密钥作为内容密钥。

（2）客户端从客户端许可证书中取出授权服务器的公钥。

（3）客户端使用服务器的公钥加密内容密钥，使用服务器的公钥所加密的内容密钥只能由服务器的私钥所解密。

（4）客户端使用客户端许可证书的公钥对内容密钥再进行一次加密，会再次获得一个加密后的对称密钥。需要注意，离线发布和在线发布所不同的是：在离线发布过程中，对内容进行了两次加密。

（5）两次加密后的对称密钥同时被放到发布许可中。

（6）客户端使用权限管理账户证书中的私钥解密客户端许可证书中的私钥。

（7）客户端使用 CLC 的私钥签署发布许可。

（8）支持 AD RMS 的应用程序将发布许可合并到受保护的文档中。

4. 受保护文档的使用过程

使用受保护文档的具体过程如下。

（1）客户端将权限管理账户证书和文档的发布许可发送到颁发发布许可的授权服务器。

（2）授权服务器使用它的私钥解出发布许可中的内容密钥。

（3）授权服务器使用权限管理账户证书中用户的公钥加密内容密钥。

（4）把加密的内容密钥和用户的使用权限添加到使用许可。

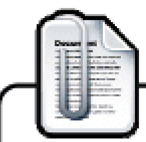
（5）授权服务器使用它的私钥签署使用许可。

（6）作为响应将该使用许可发送给客户端。

（7）密码箱使用计算机的私钥解密保存在权限管理账户证书中的用户私钥。

（8）密码箱使用用户的私钥解密内容密钥。

（9）密码箱使用内容密钥解密被加密的受保护内容。



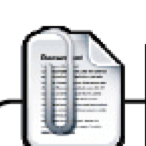
注 意

使用服务器的公钥所加密的内容只能由服务器的私钥来解开。

9.1.3　AD RMS 服务器软件需求

AD RMS 服务器端的软件需求如下：

- 必须是域的额外域控制器或域成员服务器。
- 安装 IIS 服务和 ASP.Net 组件。
- 安装 MSMQ（消息队列）服务。
- 可选数据库。如果想要创建 AD RMS 服务器群集，需要安装 SQL Server 数据库服务器或 MSDE 数据库（建议选择 SQL Server），也可以直接使用 AD RMS 自带的本地数据库。



提 示

AD RMS 服务器软件需要提前安装的 Windows 组件，在安装过程中可以自动提前安装，用户也可不必一一手动准备。

9.2 AD RMS 服务器的安装和配置

Windows Server 2008 中的 AD RMS 与 Windows Server 2003 中的 RMS 最大的区别就在于，它不再是一个独立服务插件，而是成为了 Windows 的一项内建功能，并且包含了某些升级功能。安装 AD RMS 无须下载任何安装包，直接在管理服务器窗口中启动安装向导即可轻松安装。

9.2.1 准备工作

为了确保安装过程可以顺利进行，开始之前应做好如下准备工作：

- 将计算机加入到域，或者提升为域的额外域控制器，或者子域。
- 使用域用户账户登录，但不能使用 Administrator 账户。
- 选择数据库。如果要使用独立数据库，需安装 SQL Server。否则，可使用 AD RMS 的自带数据库。
- 安装之前，确认 http://uddi.microsoft.com 和 https://uddi.microsoft.com 这 2 个网站在 Internet Explorer 中被添加至“受信任的站点”或“本地 Internet”。

9.2.2 安装 AD RMS 根服务器

AD RMS 服务并不是 Windows Server 2008 R2 系统默认安装的组件，需要用户手动添加。安装向导如果检测到有未完成的准备工作，则显示提示信息，并给出解决方案，通常情况下可以自动完成必要组件的安装。

01 使用域管理员账户（默认为 Administrator，但不能使用）登录，在“Active Directory 用户和计算机”窗口中，创建一个名为 RMS 的组织单位，并在该组织单位中创建 3 个账户（如图 9-1 所示）。其中 1 个账户为 RMS-Services，需要将这个账户添加到管理员组（例如添加到 Domain Admins 组），该账户为 RMS 服务账户，另 2 个账户为普通账户，账户显示名为张三（对应账户登录名为 rms1）、李四（对应账户登录名为 rms2）。

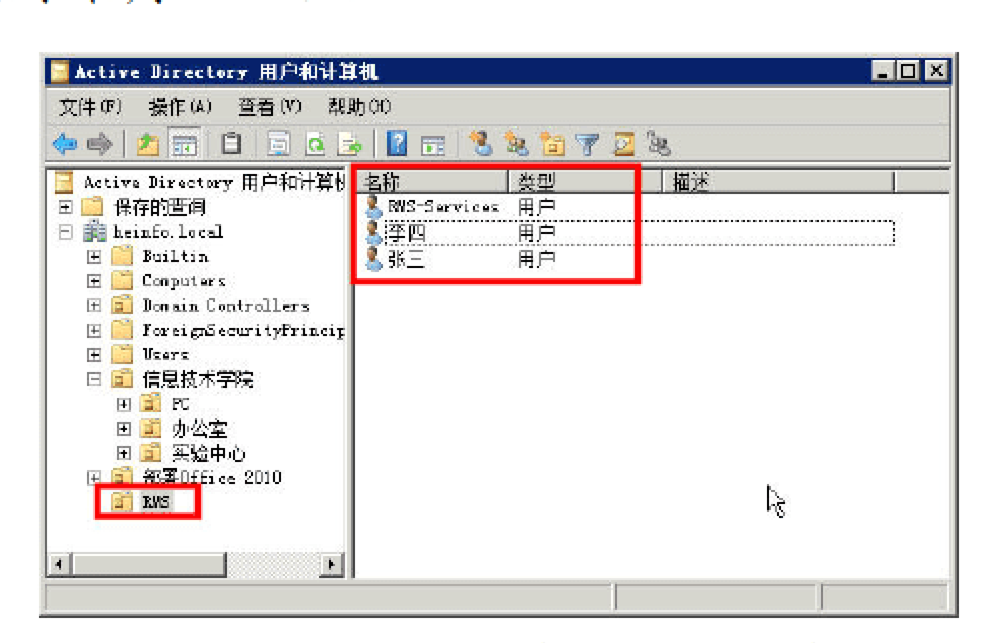


图 9-1 创建组织单位并创建账户

02 然后打开“服务器管理器”，运行“添加角色向导”，在“选择服务器角色”对话框中，选中“Active Directory Rights Management Services”复选框，则在安装 RMS 的时候会一同安装“Web 服务器（IIS）”，如图 9-2 所示。

03 在“Active Directory Rights Management Services 简介”对话框，简要介绍了 Active Directory 权限管理服务的作用以及功能，如图 9-3 所示。

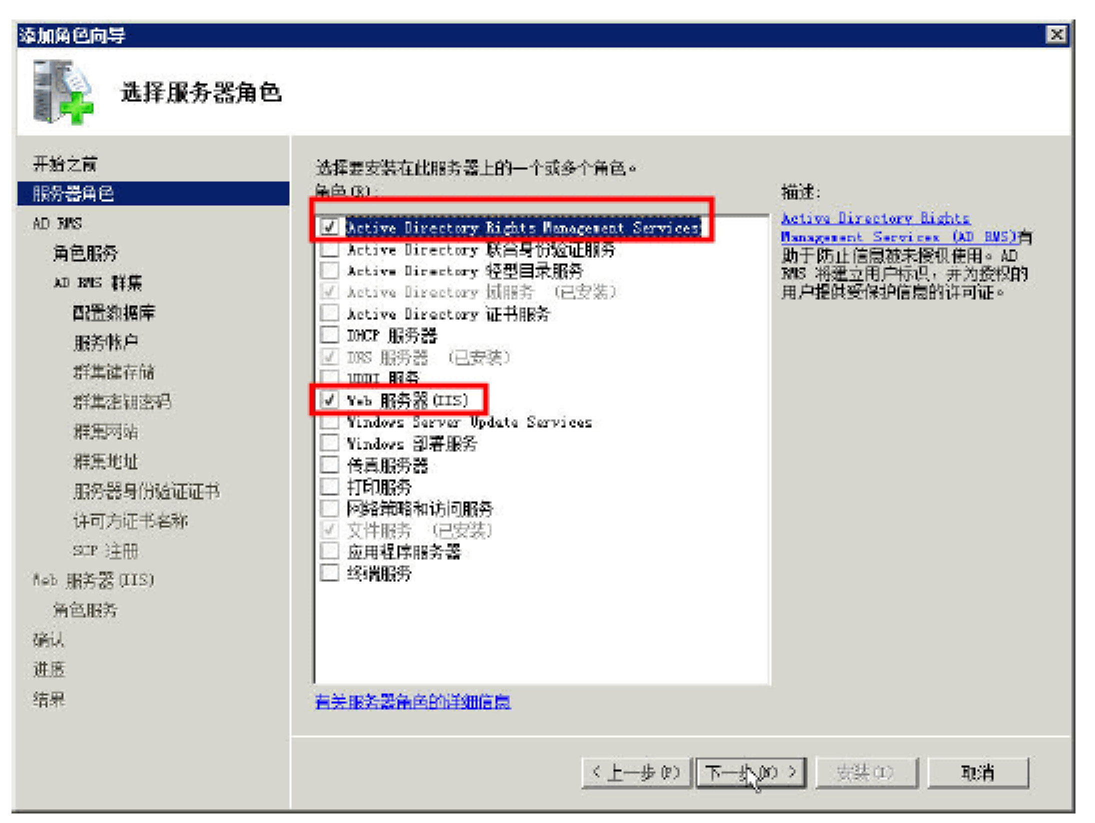


图 9-2　安装 RMS 及 IIS 服务器



图 9-3　AD RMS 简介

04 在“选择角色服务”对话框，保持默认值（Active Directory 权限管理服务器），如图 9-4 所示。

05 在“创建或加入 AD RMS 群集”对话框，选中“新建 AD RMS 群集”单选按钮，如图 9-5 所示。由于当前域中没有其他 AD RMS 群集可供加入，所以“加入现有 AD RMS 群集”单选按钮为灰色。安装完成后创建的第一台 AD RMS 服务器即为根服务器，后来加入的 AD RMS 服务器为叶服务器。

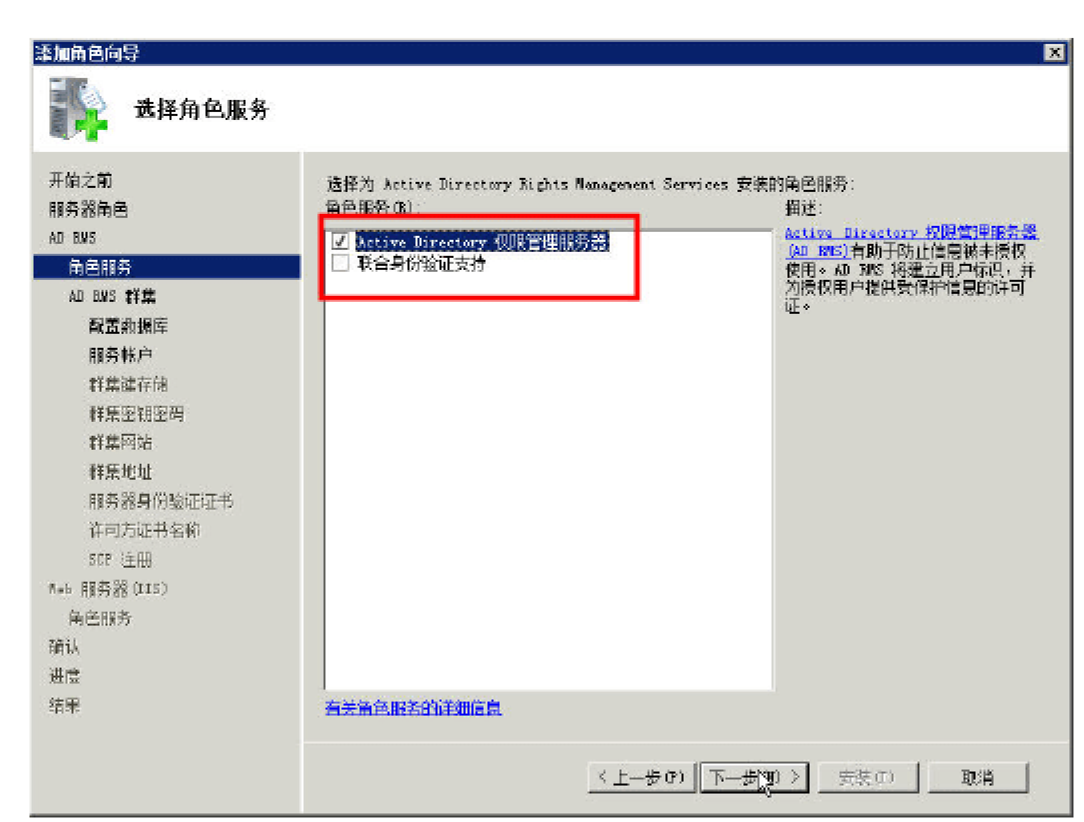


图 9-4　选择角色服务

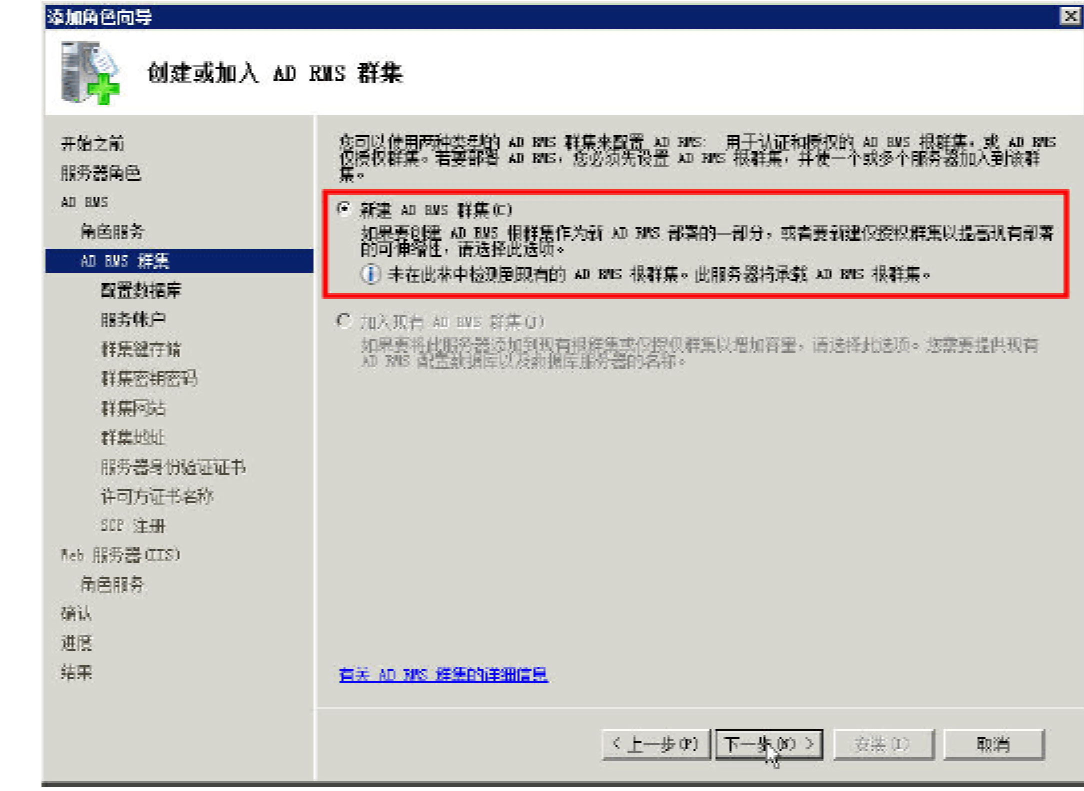
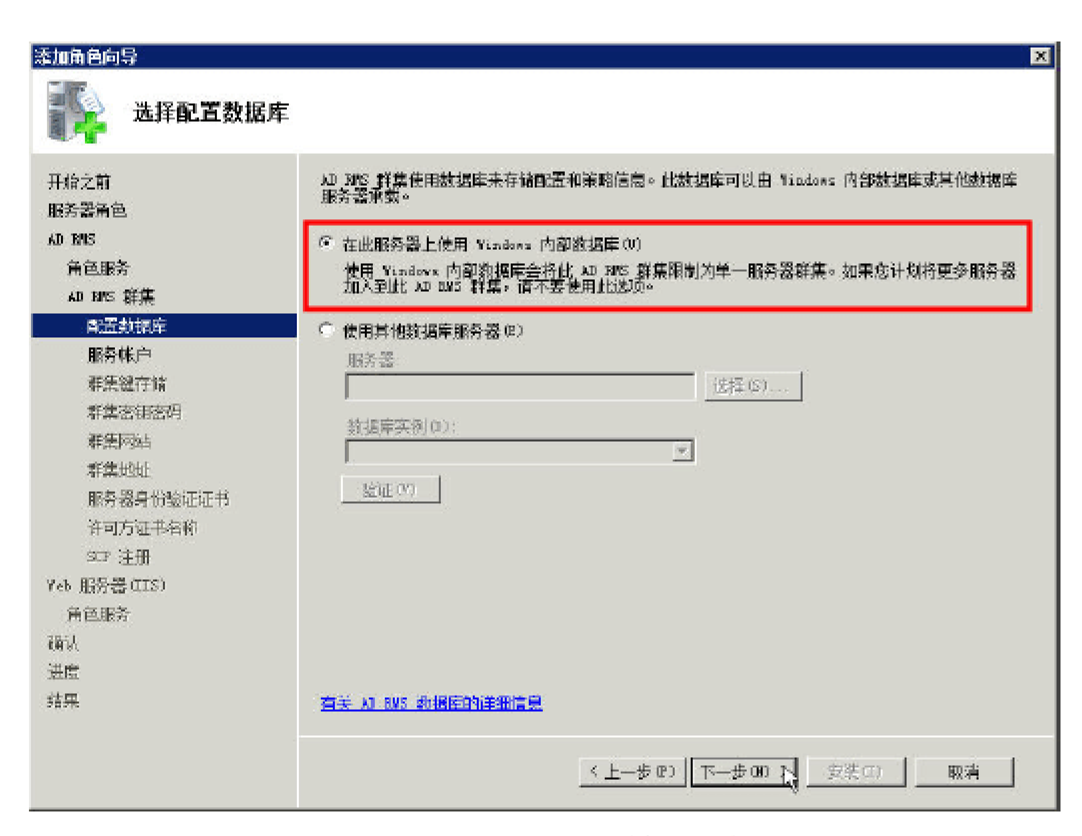


图 9-5　创建 AD RMS 群集

06 在“选择配置数据库”对话框，选中“在此服务器上使用 Windows 内部数据库”单选按钮，如图 9-6 所示。

07 在“指定服务账户”对话框，单击“指定”按钮，在弹出的对话框中，输入账户名 rms-services 及密码，然后单击“确定”按钮，如图 9-7 所示。



9-6 选择配置数据库

图 9-7 指定服务账户

08 在“配置 AD RMS 群集键存储”对话框，如图 9-8 所示。默认选择“使用 AD RMS 集中管理的密钥存储”单选按钮，即由本地服务器自动生成并存储密钥，该密钥主要用于当前根服务器以及将来叶服务器的灾难恢复，必须牢记。而“使用 CSP 密钥存储”选项则需要由专用加密服务器产生并保管该密钥，比较繁琐，但安全性也相对较高。

09 在“指定 AD RMS 群集密钥密码”对话框，设置其他 AD RMS 服务器加入群集时要使用的密码，必须妥善保存并记住该密码，如图 9-9 所示。

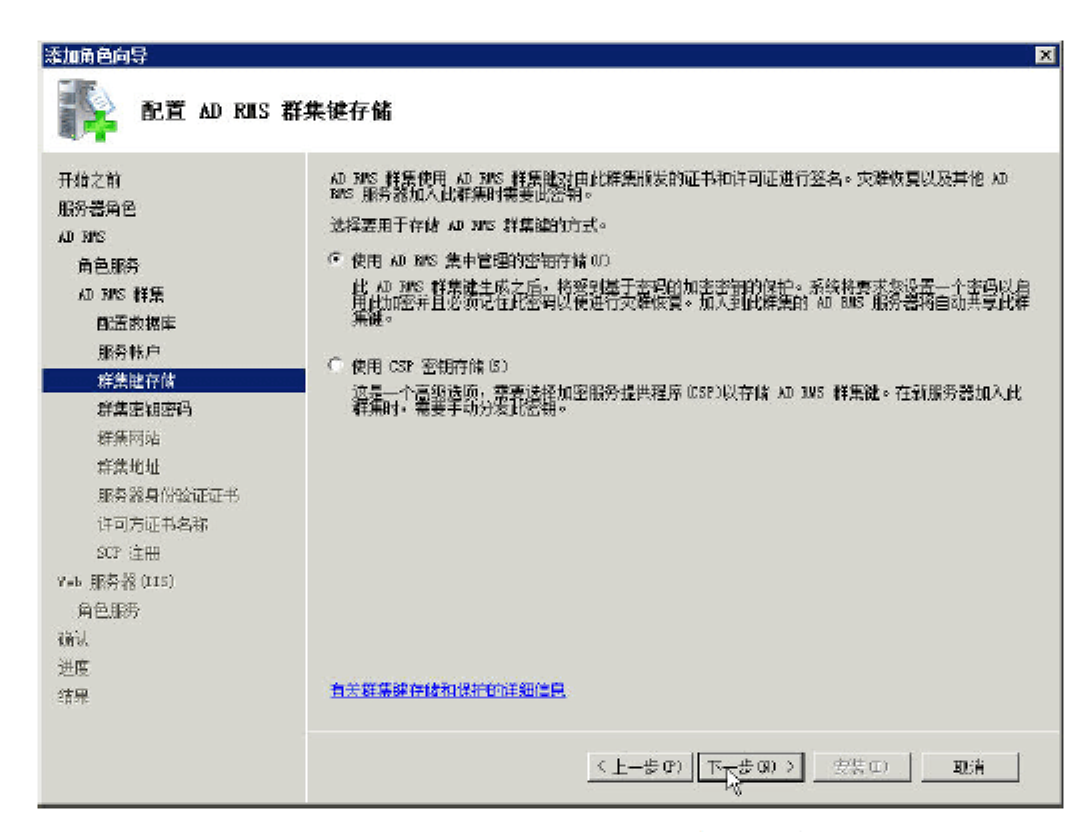


图 9-8 配置 AD RMS 群集键存储

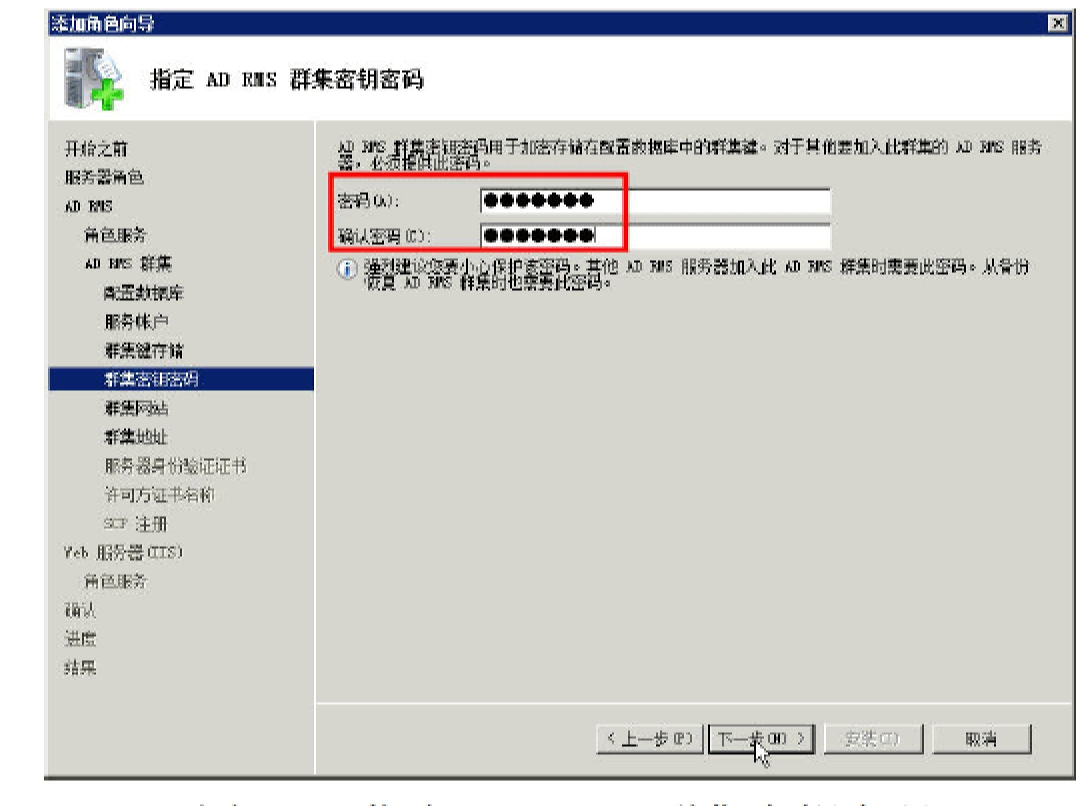


图 9-9 指定 AD RMS 群集密钥密码

10 在“选择 AD RMS 群集网站”对话框，选择管理 AD RMS 群集服务器时使用的站点，在准备工作中必须安装 IIS 就是为了在本地创建该站点，保持默认即可，如图 9-10 所示。

11 在“指定群集地址”对话框，选择“使用 SSL 加密的连接”单选按钮，并在“内部地址”文本框中输入当前服务器的 DNS 名称，在本例中为 dc.heinfo.local，然后单击“验证”按钮，验证之后才可以进行下一步的安装，如图 9-11 所示。

12 在“选择 SSL 加密的服务器身份验证证书”对话框，选择 SSL 网站所使用的证书。如果网络中有“证书服务器”，可以为该网站申请一个“服务器证书”，如果网络中没有“证书服务器”，则选择“为 SSL 加密创建自签名证书”单选按钮，如图 9-12 所示。如果在图 9-11 所示对话框中，选择“使用未加密的连接”单选按钮，则不会出现图 9-12 所示的对话框。



图 9-10　选择 AD RMS 群集网站

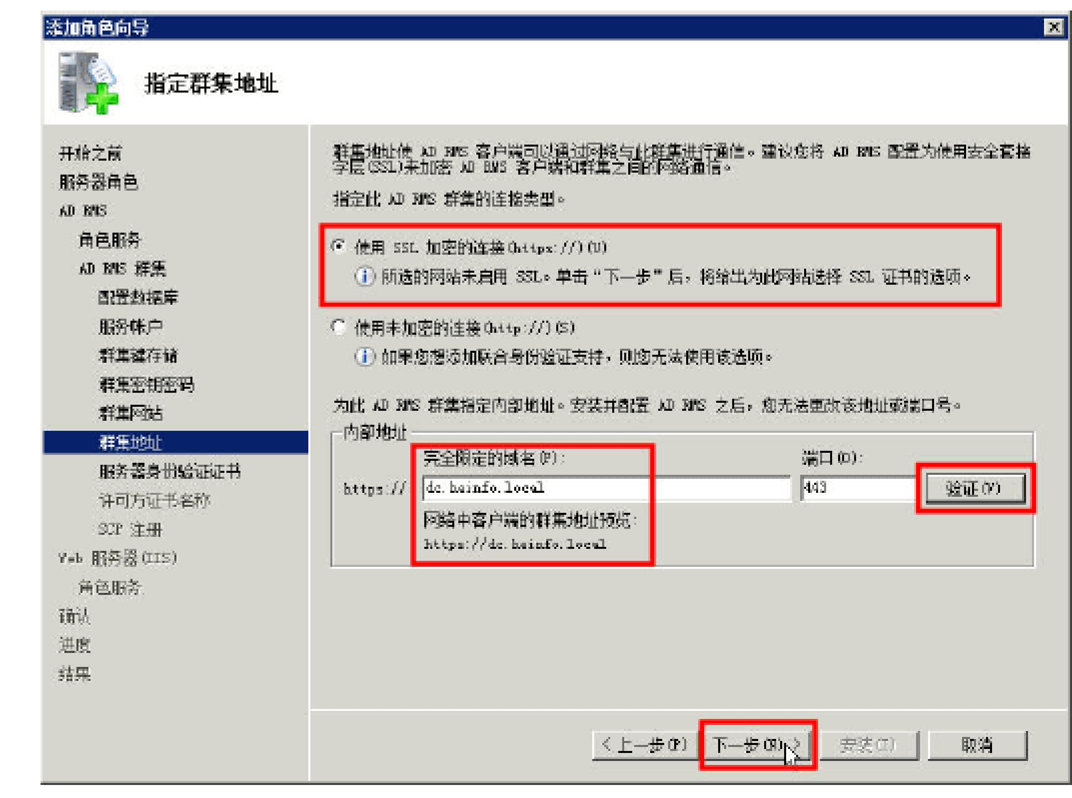


图 9-11　指定群集地址

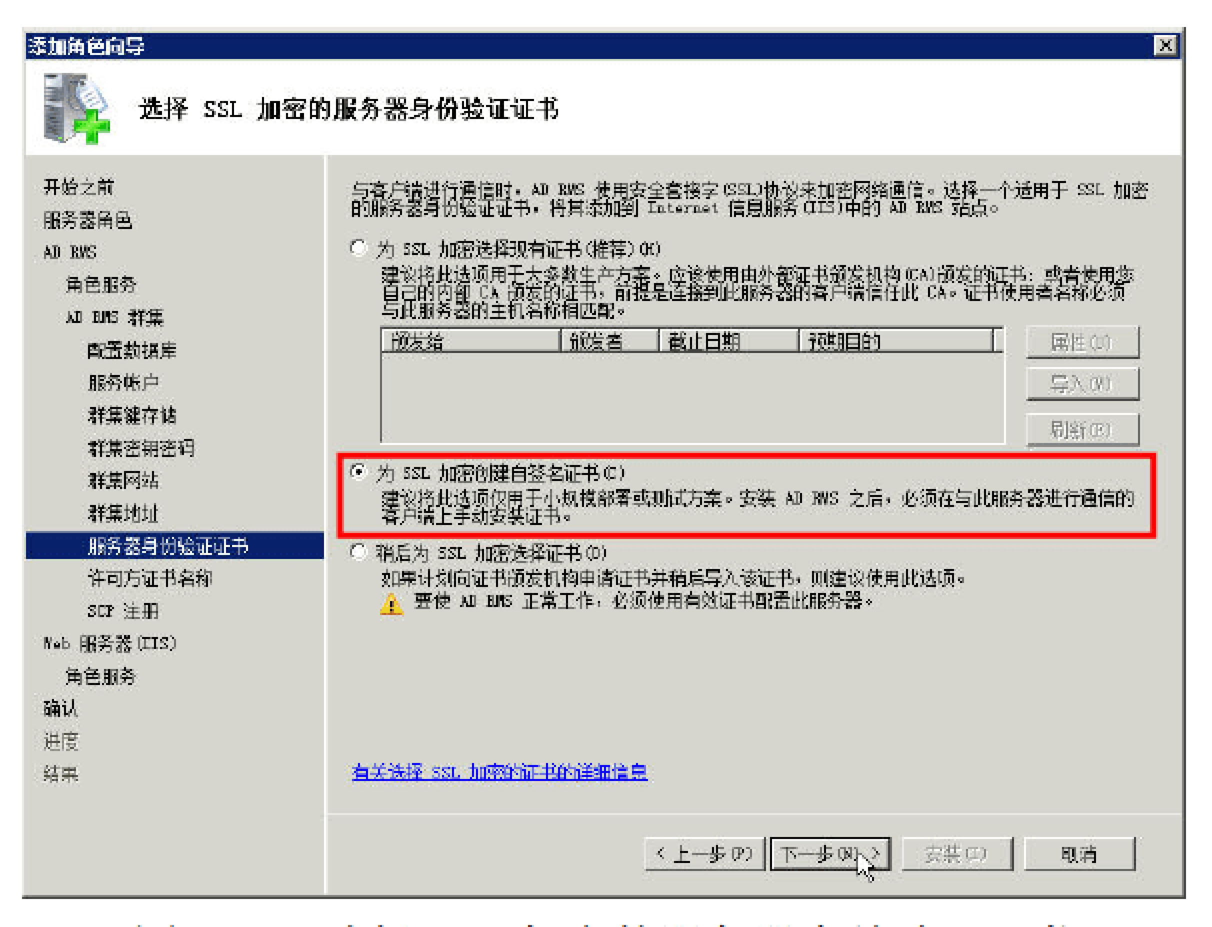


图 9-12　选择 SSL 加密的服务器身份验证证书

13 在“命名服务器许可方证书”对话框，将为 AD RMS 服务器创建一个证书，证书的名称也是服务器的计算机名称，在此修改为域的 DNS 名称 dc.heinfo.local，如图 9-13 所示。

14 在“注册 AD RMS 服务连接点”对话框，选择“立即注册 AD RMS 服务连接点”单选按钮，在安装完成后立即开始使用此 AD RMS 群集，如图 9-14 所示。



图 9-13　命名服务器许可方证书

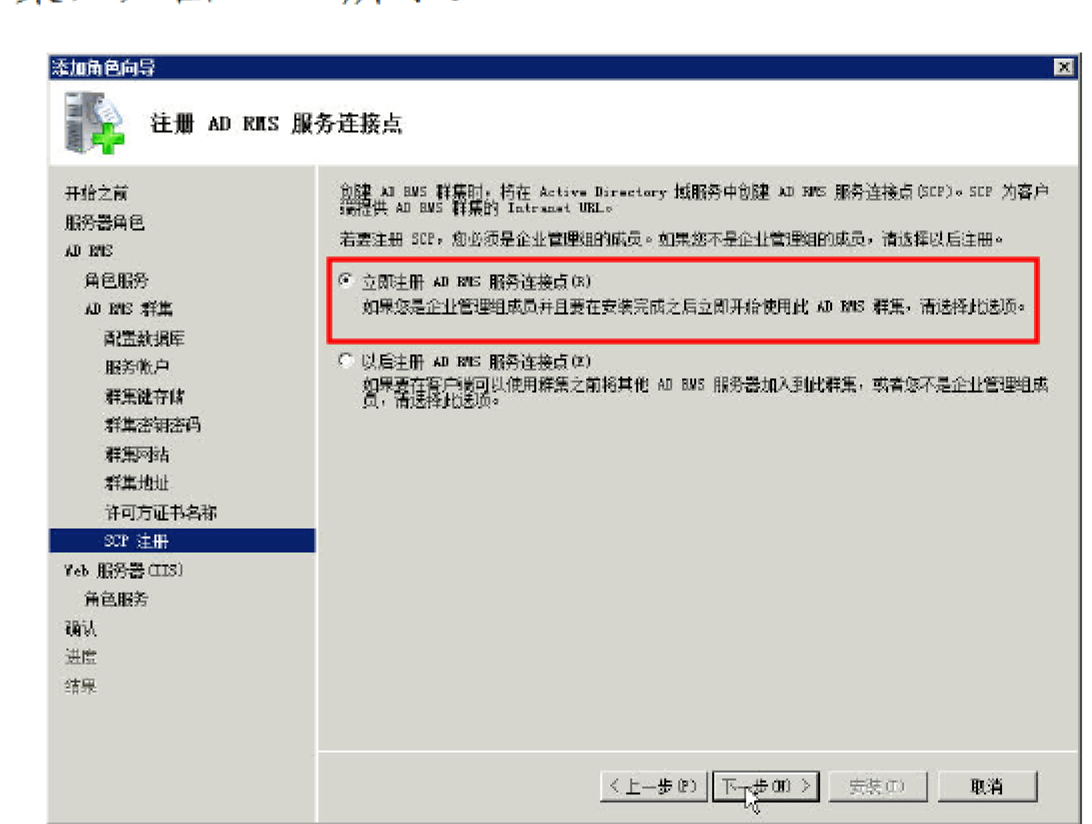


图 9-14　注册 AD RMS 服务连接点

15 在“确认安装选择”对话框，单击“安装”按钮即可开始安装，如图 9-15 所示。完成后显示如图 9-16 所示“安装结果”对话框，提示安装成功。

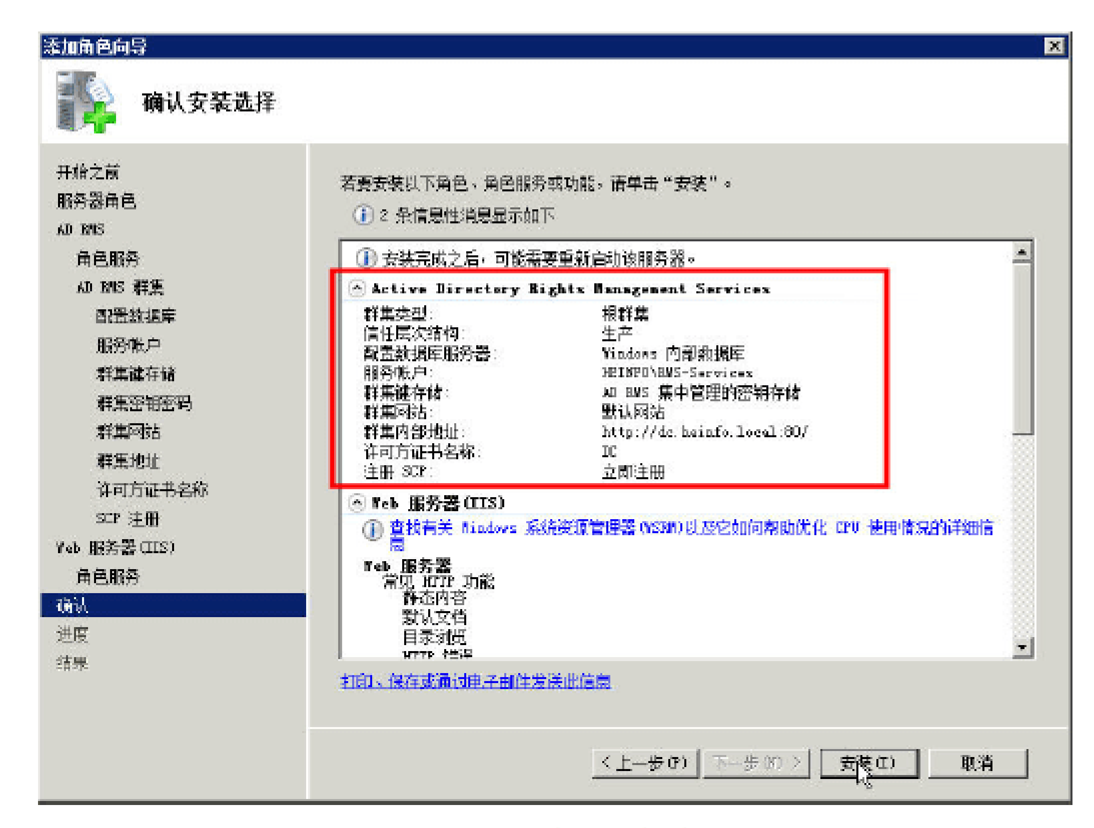


图 9-15 确认安装选择

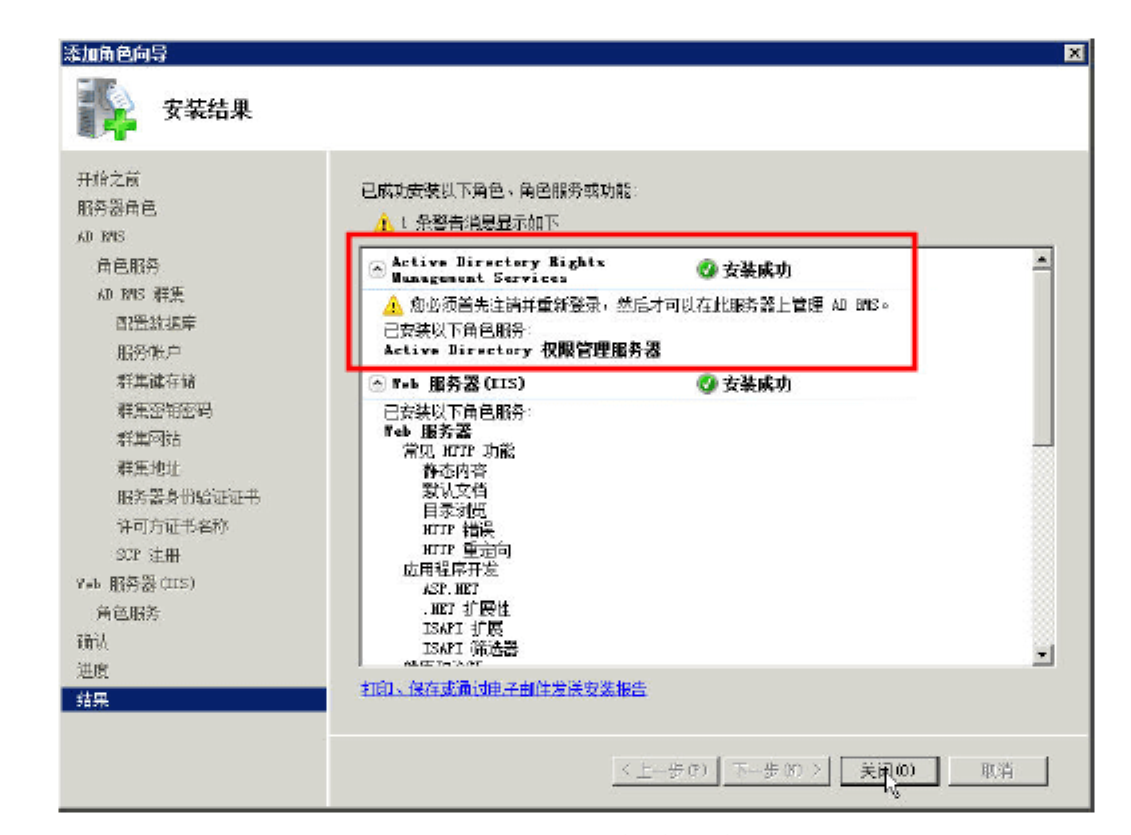
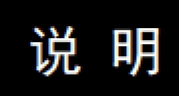


图 9-16 安装结果



说 明

如图 9-16 所示，提示用户在安装成功之后，必须“注销”并重新登录，才可以管理 AD RMS。所以，须注销当前管理员账户并重新登录，等再次登录之后继续下面的操作。如果安装 AD RMS 服务器时出现错误，可参照本文后面“9.6 卸载 AD RMS 服务器端”节的内容，在卸载 AD RMS 服务器及 Web 服务器之后，再次安装，直到安装成功。

9.2.3 添加 AD RMS 服务器群集

在第一次使用 AD RMS 服务器时，需要配置 AD RMS 服务器群集，步骤如下。

01 打开“服务器管理器”窗口，定位到“角色→Active Directory Rights Management Services”，在右侧的“详细警告信息”窗格中单击“刷新”按钮，如图 9-17 所示。

02 在“指定连接的用户密码”对话框，确认在“连接协议”选项组中，“URI 方”下拉列表中选择的是 HTTPS，“端口号”微调按钮处是 443，然后单击“完成”按钮，如图 9-18 所示。

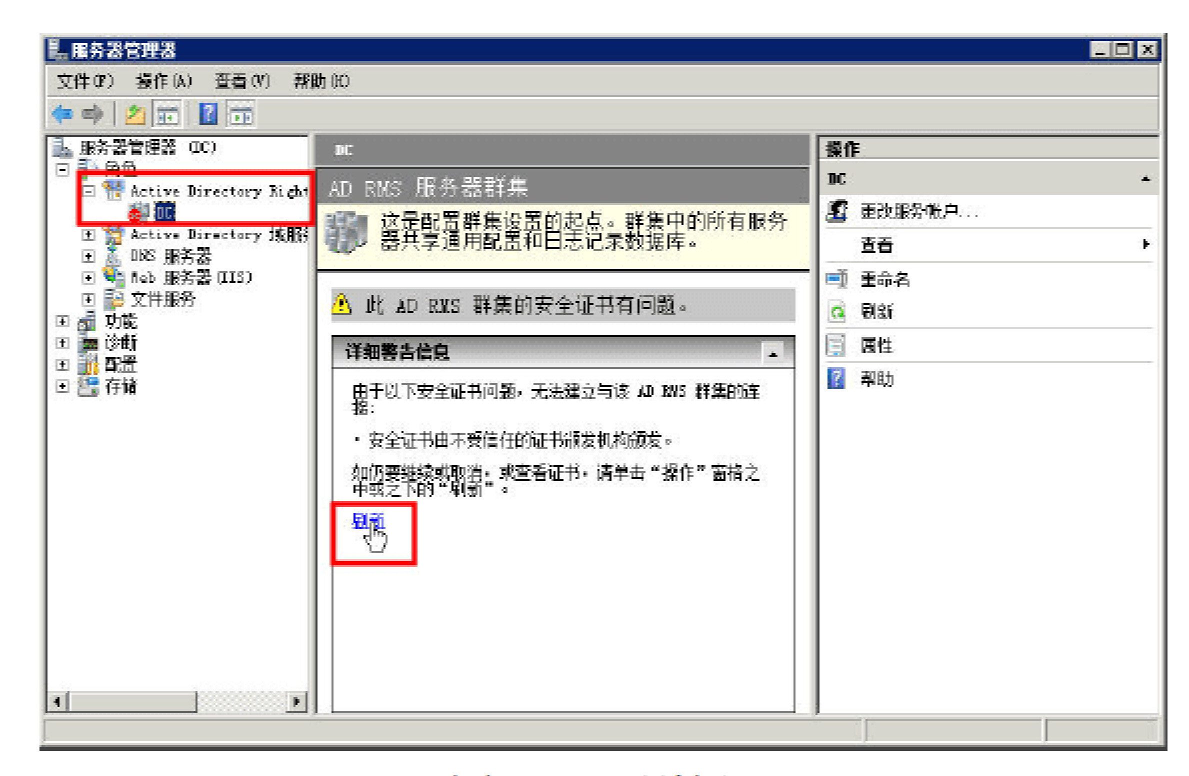


图 9-17 刷新

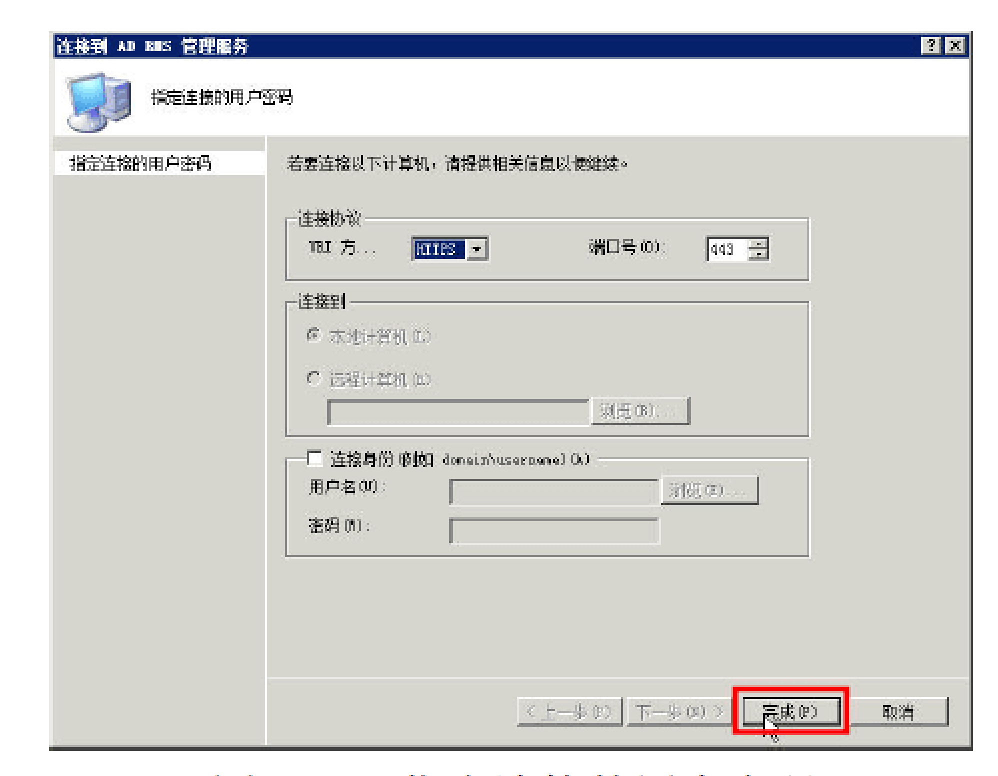


图 9-18 指定连接的用户密码

03 在弹出的“安全警报”对话框中单击“查看证书”按钮，如图 9-19 所示。

04 由于我们选择的是“自签名证书”，所以该证书的“根目录证书”不受信任。为了避免每次连接 AD RMS 群集时出现图 9-20 的提示，我们可以将自签名的“根目录证书”添加到本地信任列表中。在“证书”对话框中单击“安装证书”按钮，如图 9-20 所示。

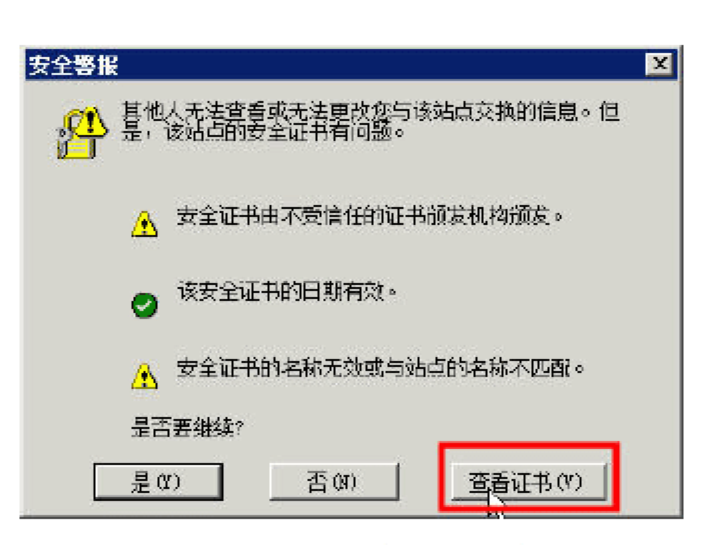


图 9-19　查看证书

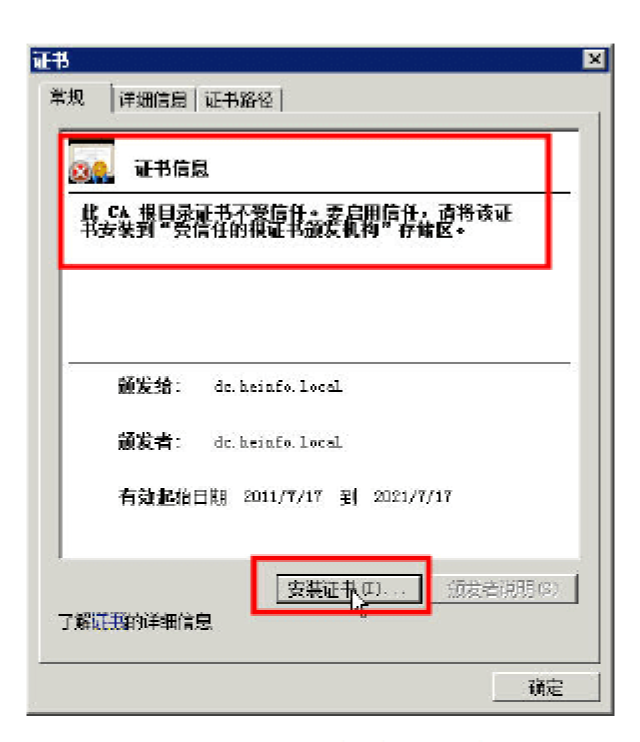


图 9-20　安装证书

05 在“证书存储”对话框中，选择“将所有的证书放入下列存储”单选按钮，单击“浏览”按钮，在弹出的“选择证书存储”对话框中，选择“受信任的根证书颁发机构”选项，然后单击“确定”按钮，如图 9-21 所示。

06 在“正在完成证书导入向导”对话框中，单击“完成”按钮，如图 9-22 所示。在随后弹出的“安全性警告”提示框中，单击“是”按钮。

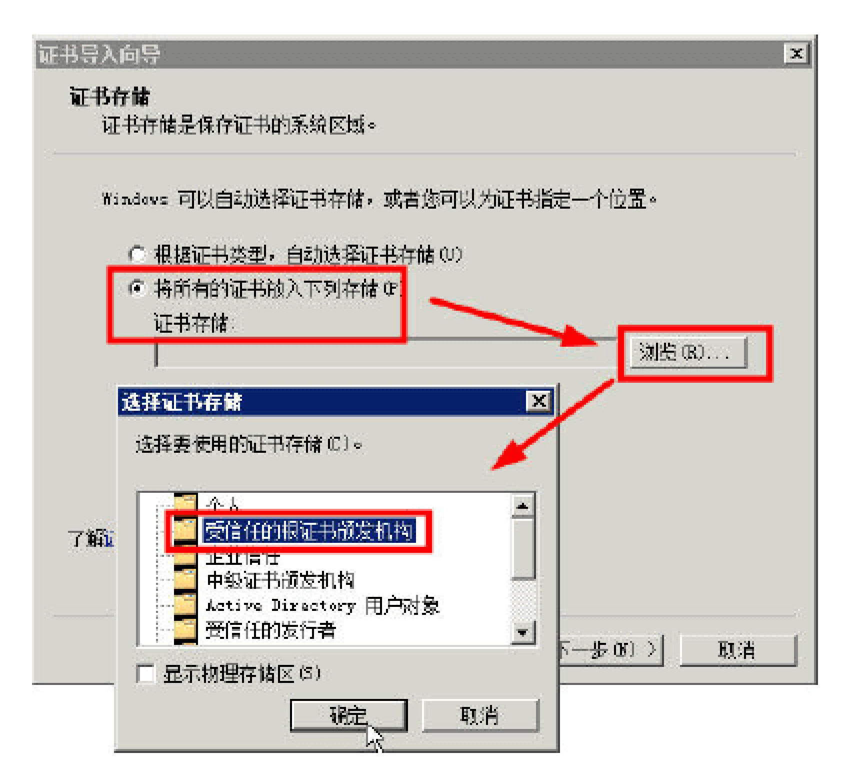


图 9-21　添加证书到受信任的根证书颁发机构

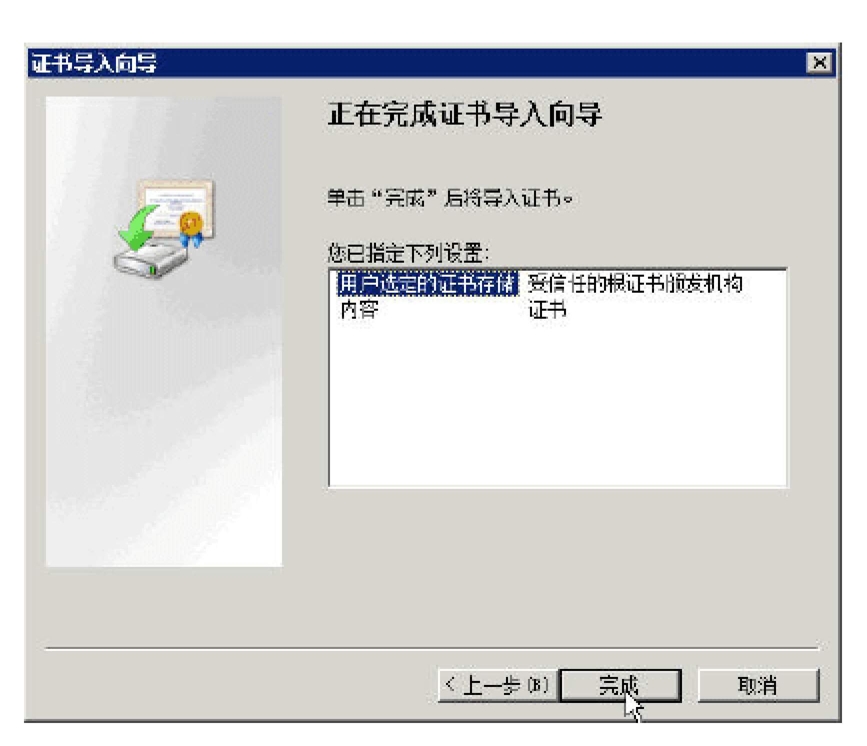


图 9-22　完成证书导入向导

07 返回到图 9-20 的“证书”对话框，单击“确定”按钮，再次返回到“安全警报”对话框，如图 9-19 所示，单击“是”按钮，完成添加 AD RMS 服务器群集，如图 9-23 所示。

添加完 AD RMS 服务器群集之后，不再需要其他配置即可使用。下面我们通过具体的实验，测试使用 AD RMS 服务器保护网络中的 Office 文档的内容。我们将使用如图 9-24 所示的网络拓扑进行测试。

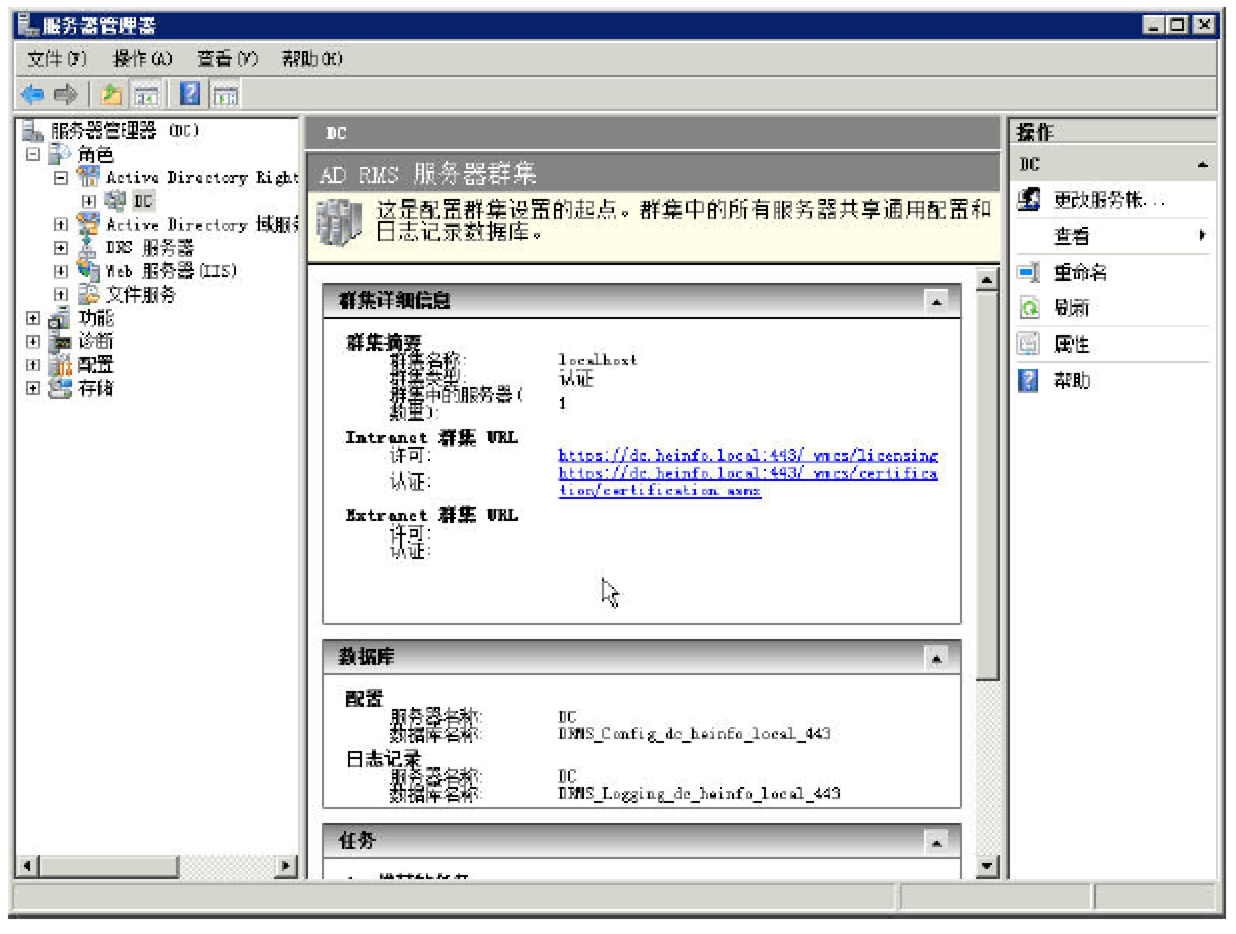


图 9-23　完成添加 AD RMS 服务器群集

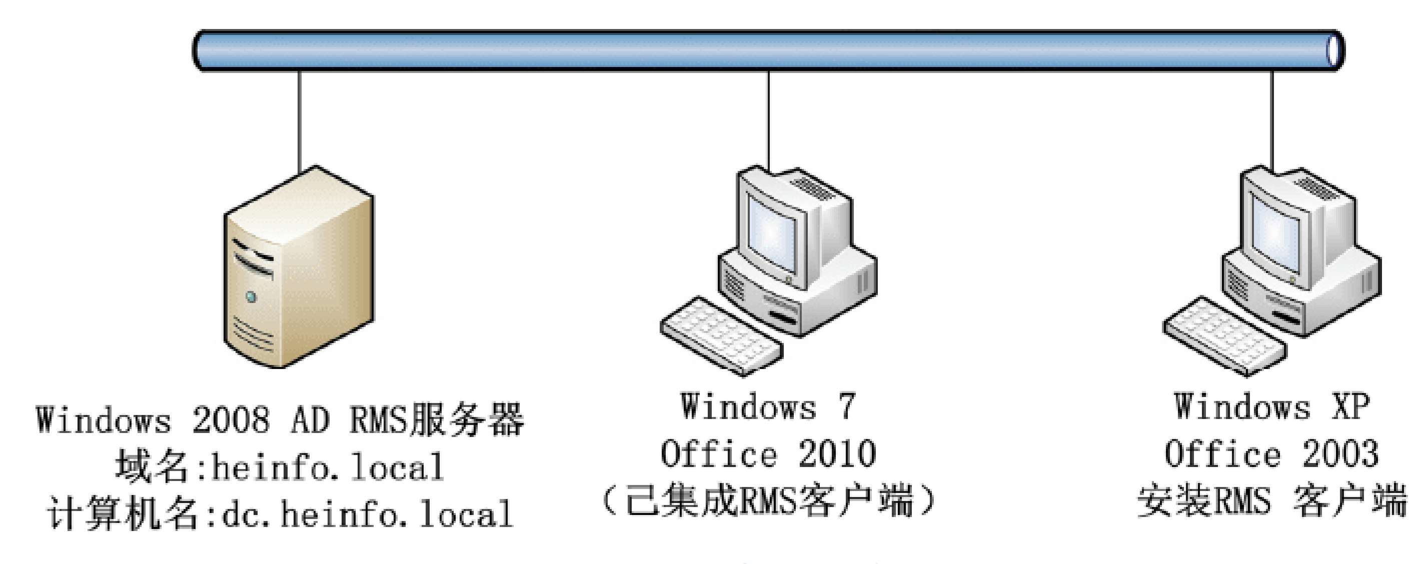


图 9-24　实验拓扑

9.2.4　添加 RMS 测试用户

为了实现图 9-24 的内容，我们需要在 Active Directory 中创建两个用户并为两个用户指定邮箱。注意，在采用 AD RMS 进行文档保护时，必须要为用户指定邮箱。在本例中，这两个用户在图 9-1 中已经创建，分别是显示名为“张三”、登录名为 rms1，显示名为“李四”、登录名为 rms2 的用户。打开“Active Directory 用户和计算机”窗口，找到这两个用户，在“常规”选项卡中分别为张三、李四指定“电子邮件”地址，张三的为 zhangsan@msft.com、李四的为 lisi@msft.com，如图 9-25、图 9-26 所示。

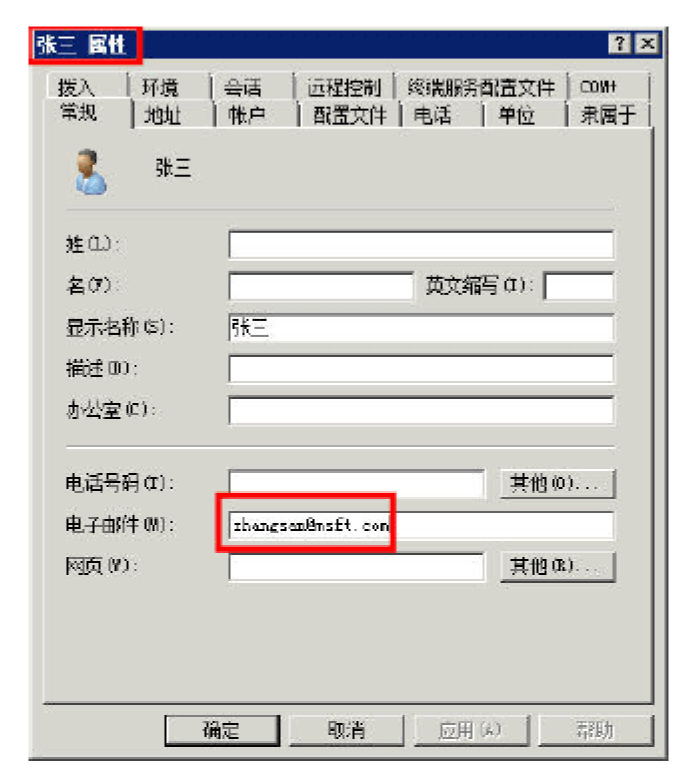


图 9-25　为张三指定邮箱

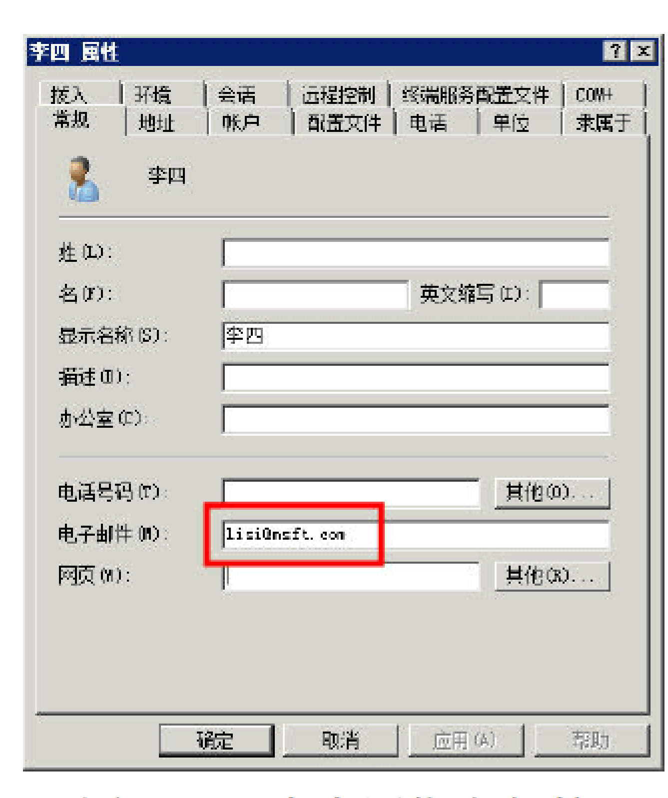


图 9-26　为李四指定邮箱

经过上述设置，就可以测试使用 AD RMS 保护文档了。我们分别在 Windows 7+Office 2010 与 Windows XP + Office 2003 上进行测试。

9.3　在 Windows 7 客户端测试 RMS

在 Office 2010 中，已经集成了 RMS 的客户端程序。默认情况下，只要打开文档，对打开的文档进行“限制”即可以体验到 RMS 功能。我们将用下面的步骤进行测试。

01 以“张三”的身份登录，对文档进行保护、限制。将文档保存在其他用户能访问的地址。

02 注销“张三”，以“李四”的身份登录，打开上一步“张三”保护的文档，看能否实现相应的功能。

9.3.1　以张三身份登录并保护文档

在已经加入到 Active Directory 的 Windows 7 中，以张三的身份登录，对一个文档进行限制，操作步骤如下。

01 以张三的身份登录（用户登录名为 rms1）到域，如图 9-27 所示。

02 用 Office 2010 打开一个文档，然后单击“文件”菜单，定位到“信息→保护文档→按人员限制权限→管理凭据”，如图 9-28 所示。




图 9-27　以张三的用户名登录

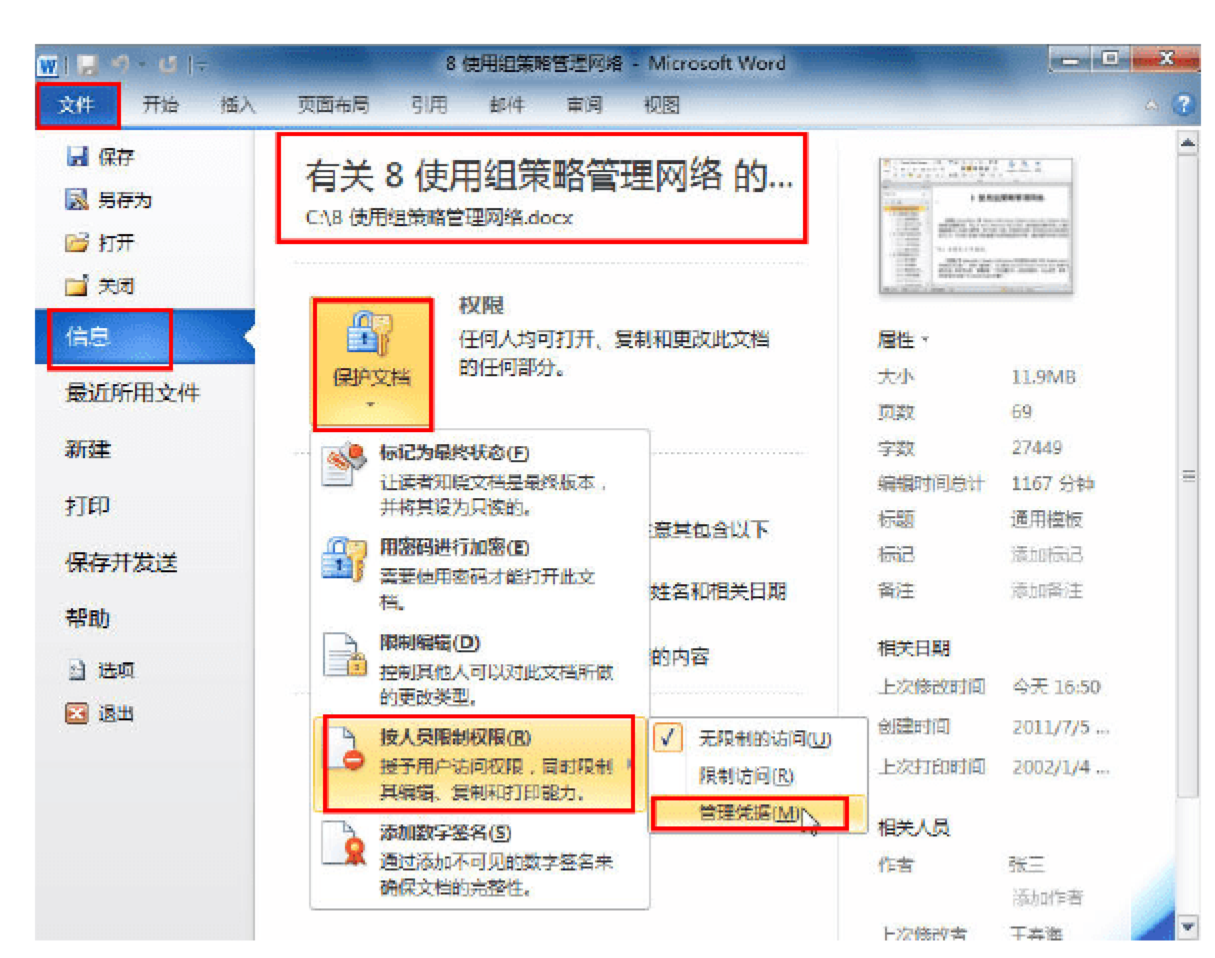


图 9-28　管理凭据

03 首先会弹出“安全警报”提示框，如图 9-29 所示。

04 出现图 9-29 的提示，仍然是证书的原因。单击“查看证书”按钮，在弹出的“证书”对话框中，在“常规”选项卡中，单击“安装证书”按钮，并将其安装到“受信任的根证书颁发机构”中，如图 9-30 所示。

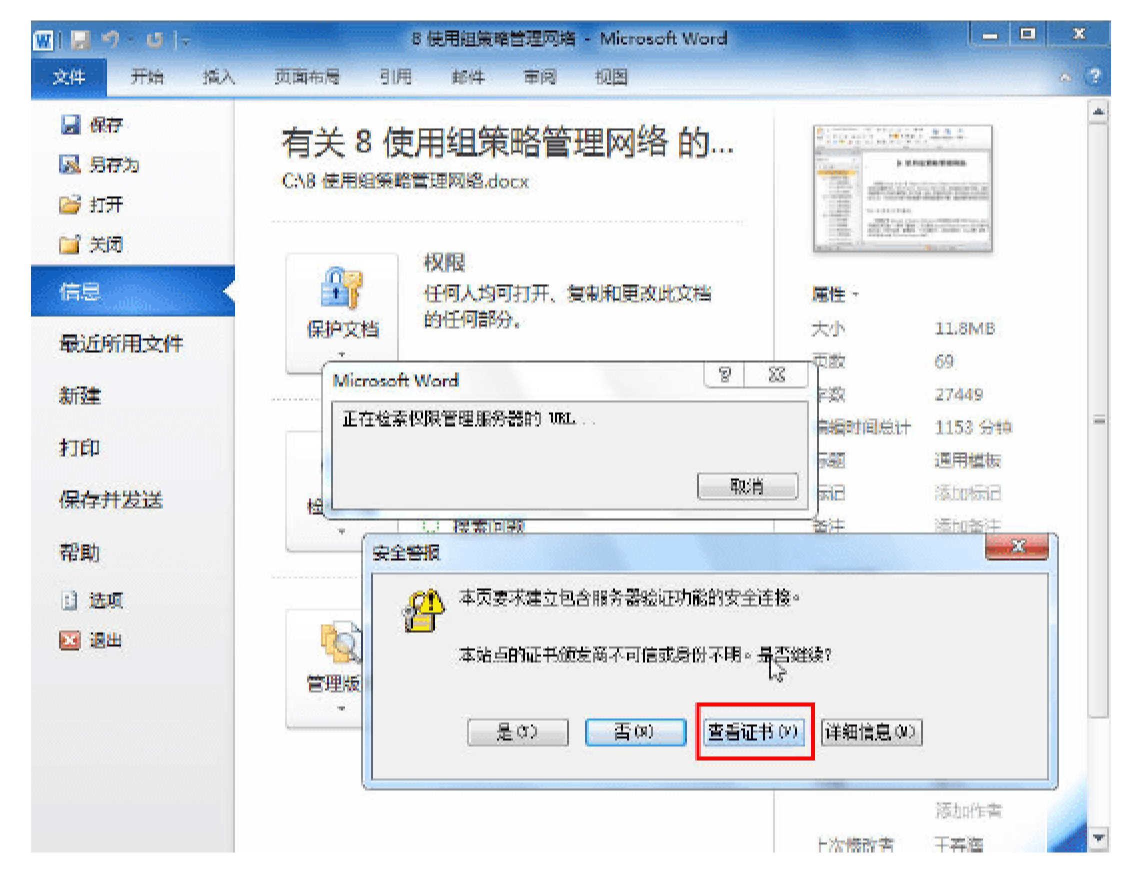


图 9-29 安全警报

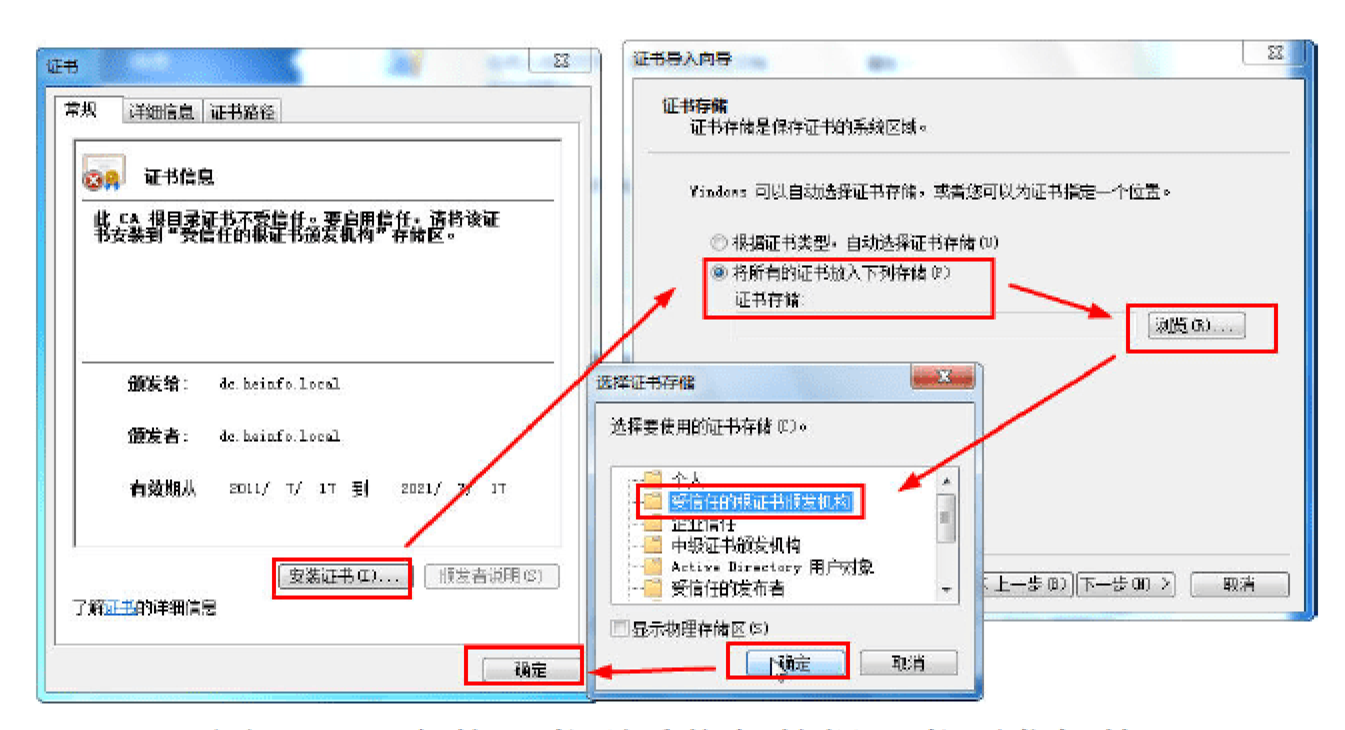


图 9-30 安装证书到受信任的根证书颁发机构

05 在弹出的“安全性警告”提示框中，单击“是”按钮，安装该证书，如图 9-31 所示。

06 返回到如图 9-29 所示的“安全警告”提示框，单击“是”按钮，以后再使用该用户名登录时，将不会出现该提示。

07 在弹出的“Windows 安全”对话框中，使用“张三”的用户名 rms1 及密码登录，并选中“记住我的凭据”复选框，如图 9-32 所示。

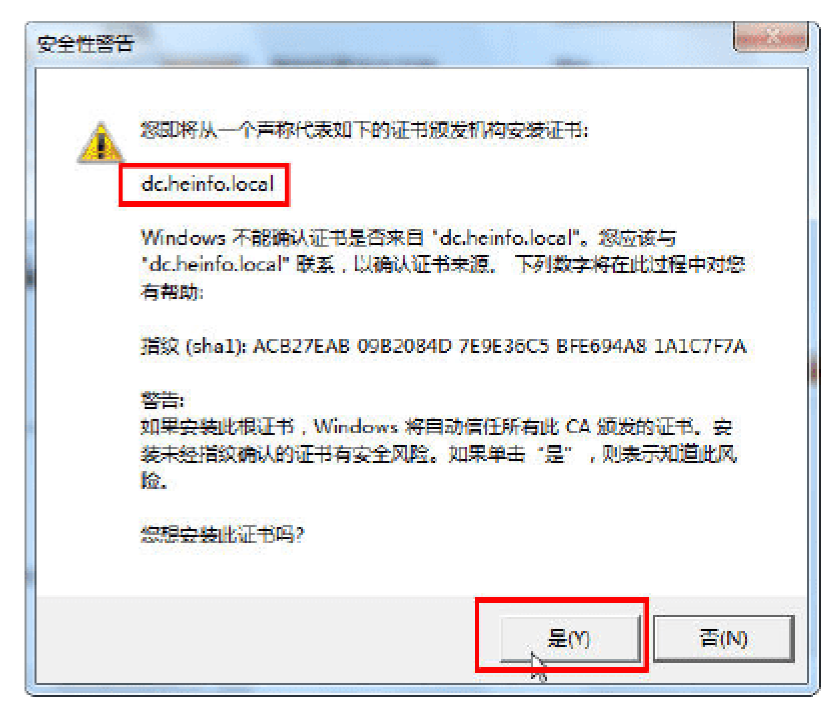


图 9-31 确认安装根证书

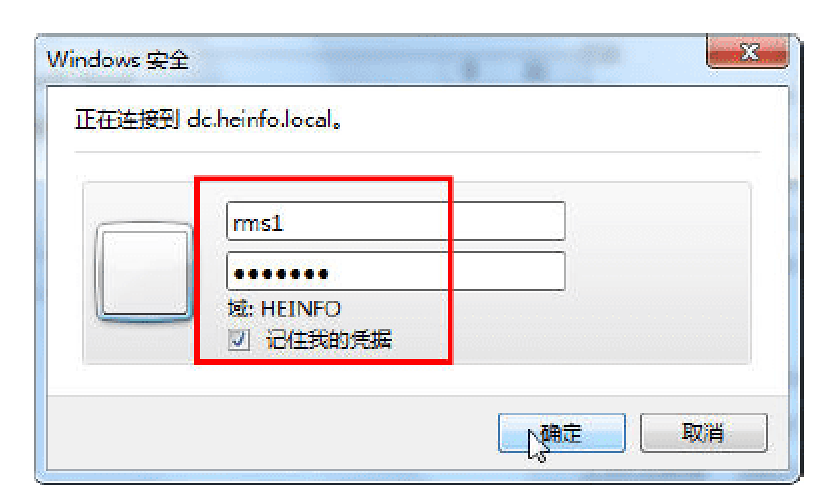


图 9-32 输入用户名与密码

08 在“选择用户”对话框中，选中“始终使用此账户”复选框，如图 9-33 所示。

09 在“权限”对话框中，选中“限制对此文档的权限”复选框，分别有“读取”与“更改”

权限。如果要添加用户的权限，可以在“读取”与“更改”文本框中，分别输入要添加的用户（添加用户对应的邮箱，在类似图 9-25、图 9-26 中指定的邮箱）；如果要允许“所有人”，请单击“ ”按钮添加，如图 9-34 所示，在“读取”列表中添加了“所有人”。然后，单击“其他选项”按钮。

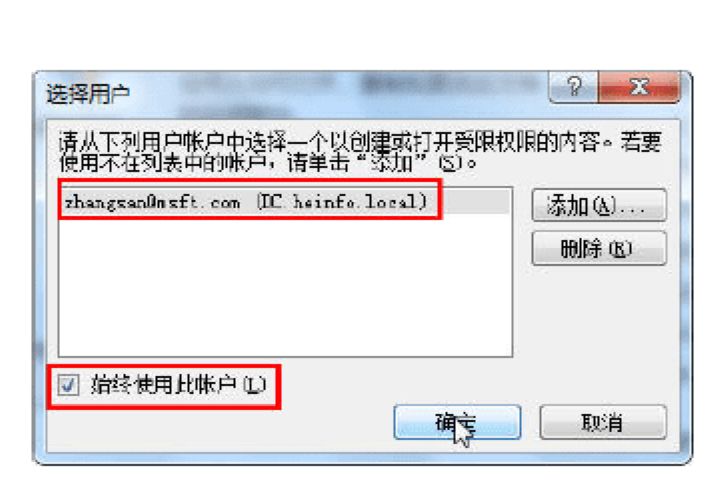


图 9-33 始终使用此账户

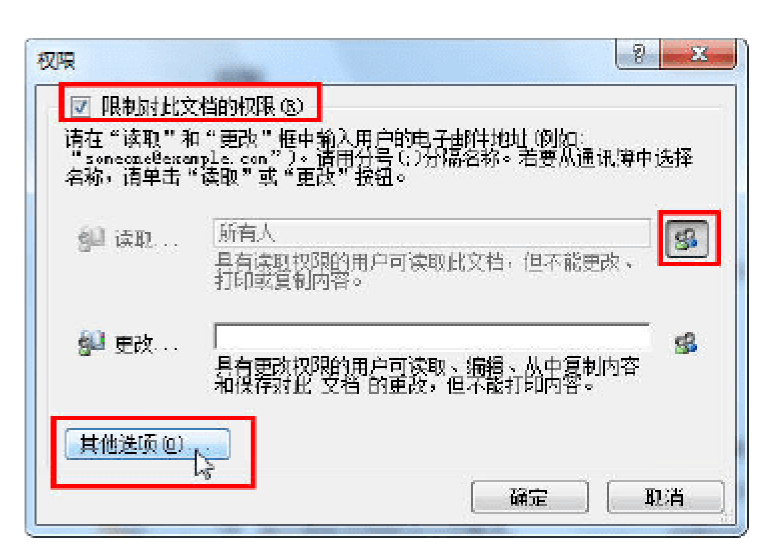


图 9-34 权限

10 在弹出的“权限”对话框中，在“以下用户具有访问此文档的权限”列表框中，显示了允许的用户及对应的权限。如果要更改权限，在“访问级别”列表中，选中一个权限再单击即出现修改下拉按钮。在“用于用户的附加权限”选项组中，列出了其他的权限。例如，如果选中“此文档的到期日期为”复选框，将限制文档的使用期限，当时间到达此指定期限后（以 Active Directory 域服务器时间为准），除了“完全控制”权限的所有者，其他用户将不能打开该文档。如果选中“打印内容”复选框，则允许用户使用“打印机”将该文档打印出来，如图 9-35 所示。

11 如果要添加其他用户，则在图 9-35 中单击“添加”按钮，在弹出的“添加用户”对话框中，以邮箱的格式添加其他用户，在此添加 lisi@msft.com，如图 9-36 所示。

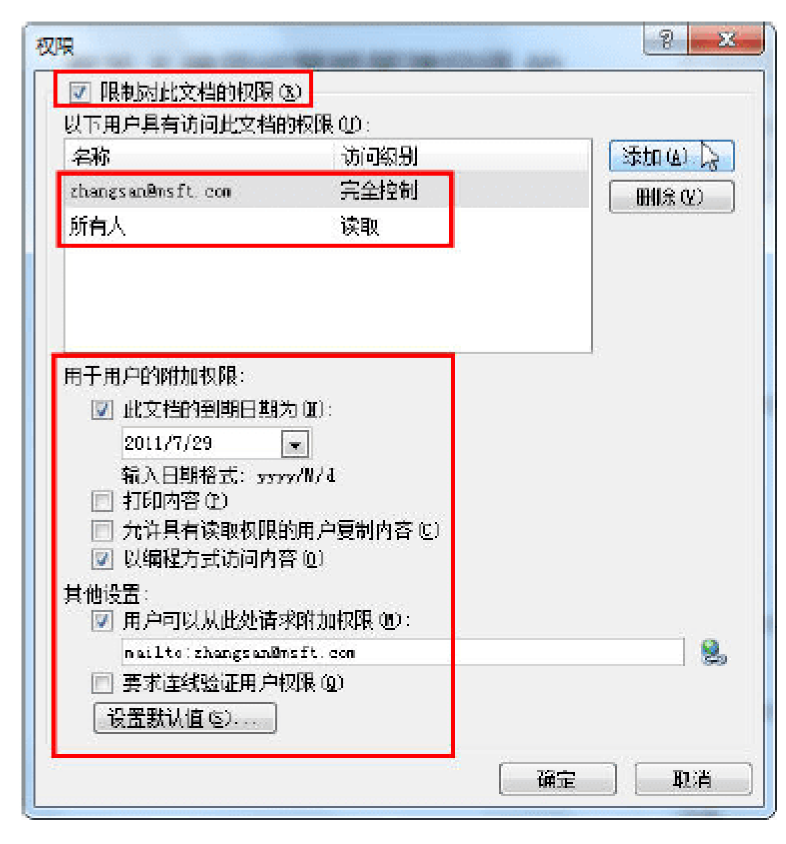


图 9-35 权限

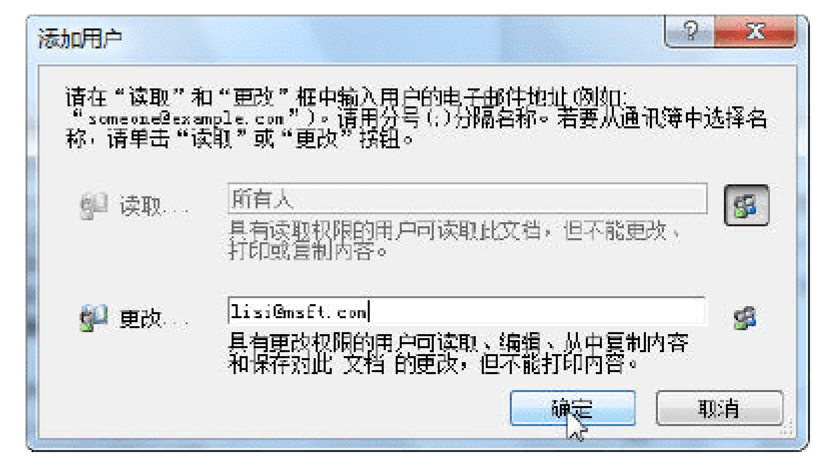
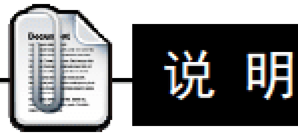


图 9-36 添加用户

如果要添加多个用户，须用逗号“,”分隔。

12 添加之后，返回到“权限”对话框，在“访问级别”列表中，修改用户的访问权限。可以在“读取、更改、完全控制”之间更改，如图 9-37 所示。设置之后单击“确定”按钮。



说 明

对于“用于用户的附加权限”设置，如果单击“设置默认值”按钮，则以后该用户打开其他文档进行限制时，默认将会是该设置。

13 设置权限之后，返回到“开始”选项卡，可以看到“限制访问”的提示，如图 9-38 所示。

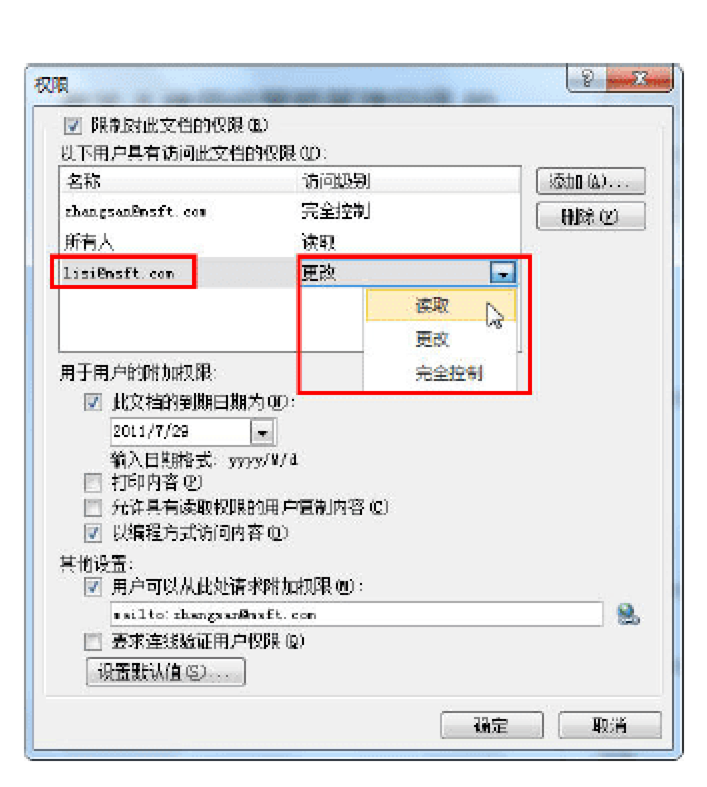


图 9-37　更改权限

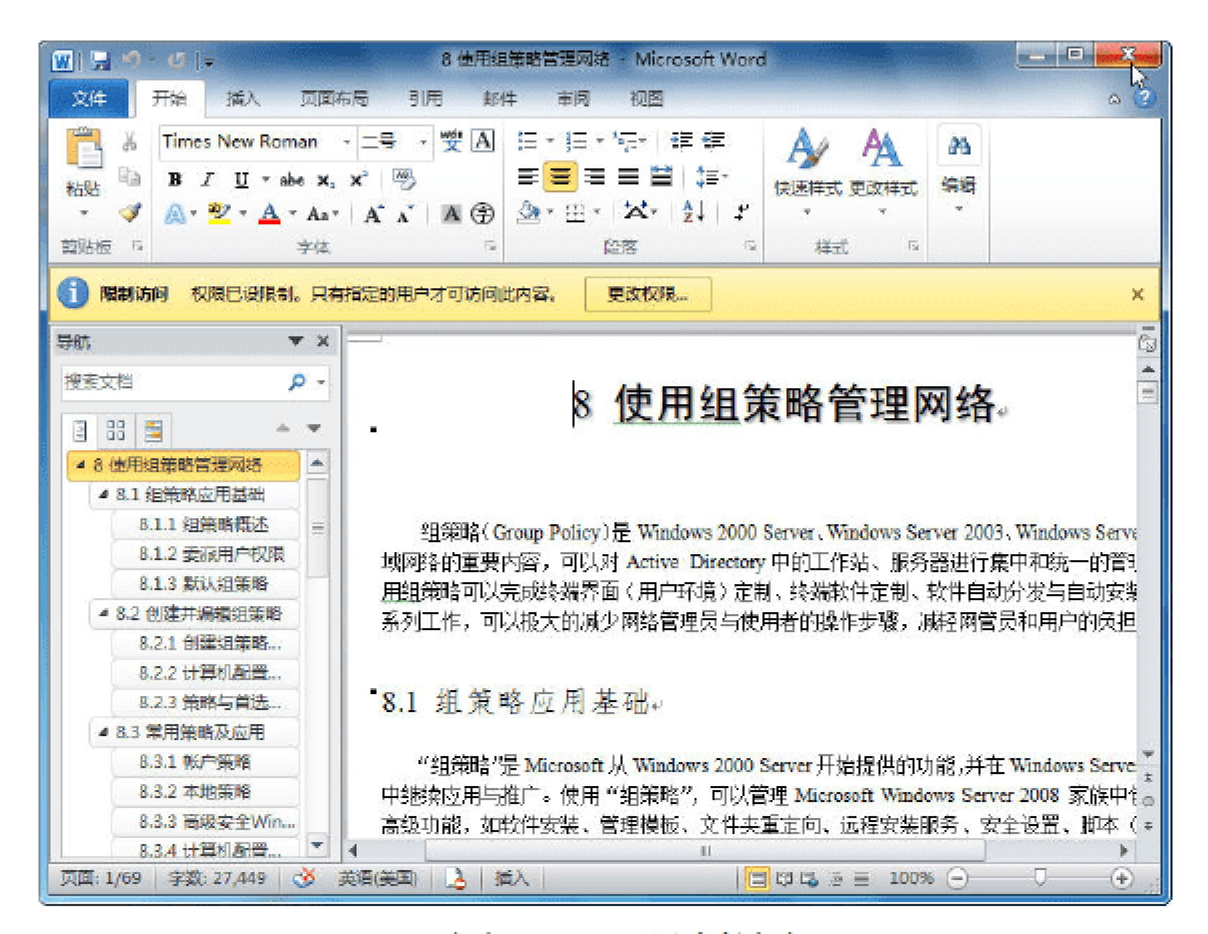


图 9-38　限制访问

然后将该文档保存到 C 盘根目录，注销“张三”用户。接下来为使用“李四”用户查看受保护的文档。

9.3.2　以李四身份登录并查看受保护文档

本小节使用李四的身份登录，并打开图 9-38 中保存的文档，查看受 RMS 保护的文档，主要步骤如下。

01 以李四身份登录，如图 9-39 所示。

02 打开图 9-38 中保存的文档，第一次使用的时候，会出现 9.3.1 小节中图 9-29 中的提示。可按照 9.3.1 小节步骤 3～5 的操作，安装根证书，然后弹出“Windows 安全”对话框，输入李四的用户名登录，如图 9-40 所示。



图 9-39　以李四身份登录

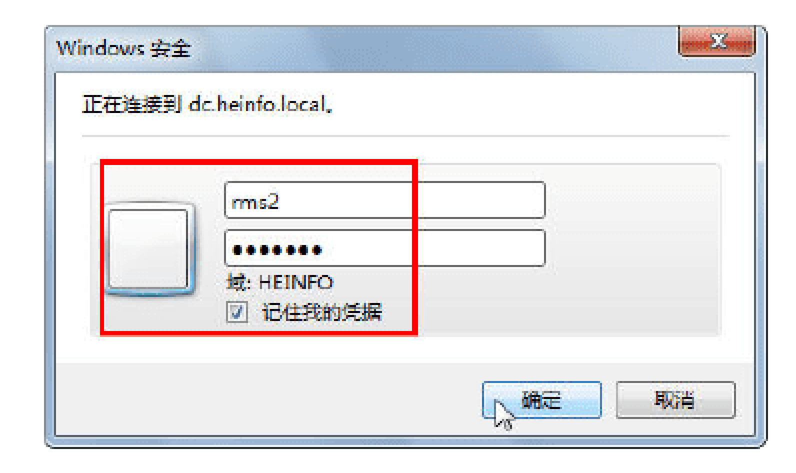


图 9-40　以 rms2 的用户名登录

03 在弹出的“Microsoft Office”对话框中，提示“此文档的权限已被限制”，选中“不再显示此消息”复选框，如图 9-41 所示。

04 打开文档之后，会弹出“限制访问”的提示，单击“查看权限”按钮，如图 9-42 所示。

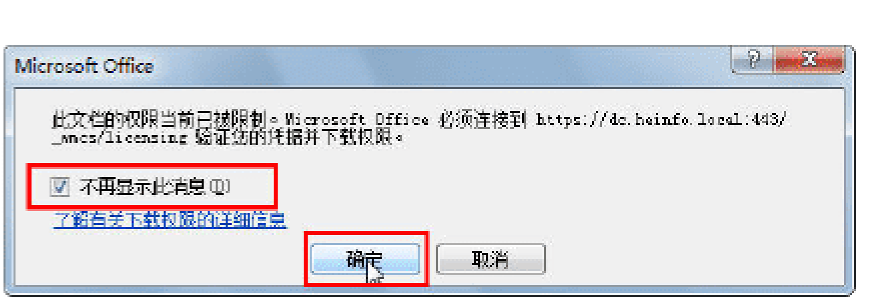


图 9-41　此文档的权限当前已被限制

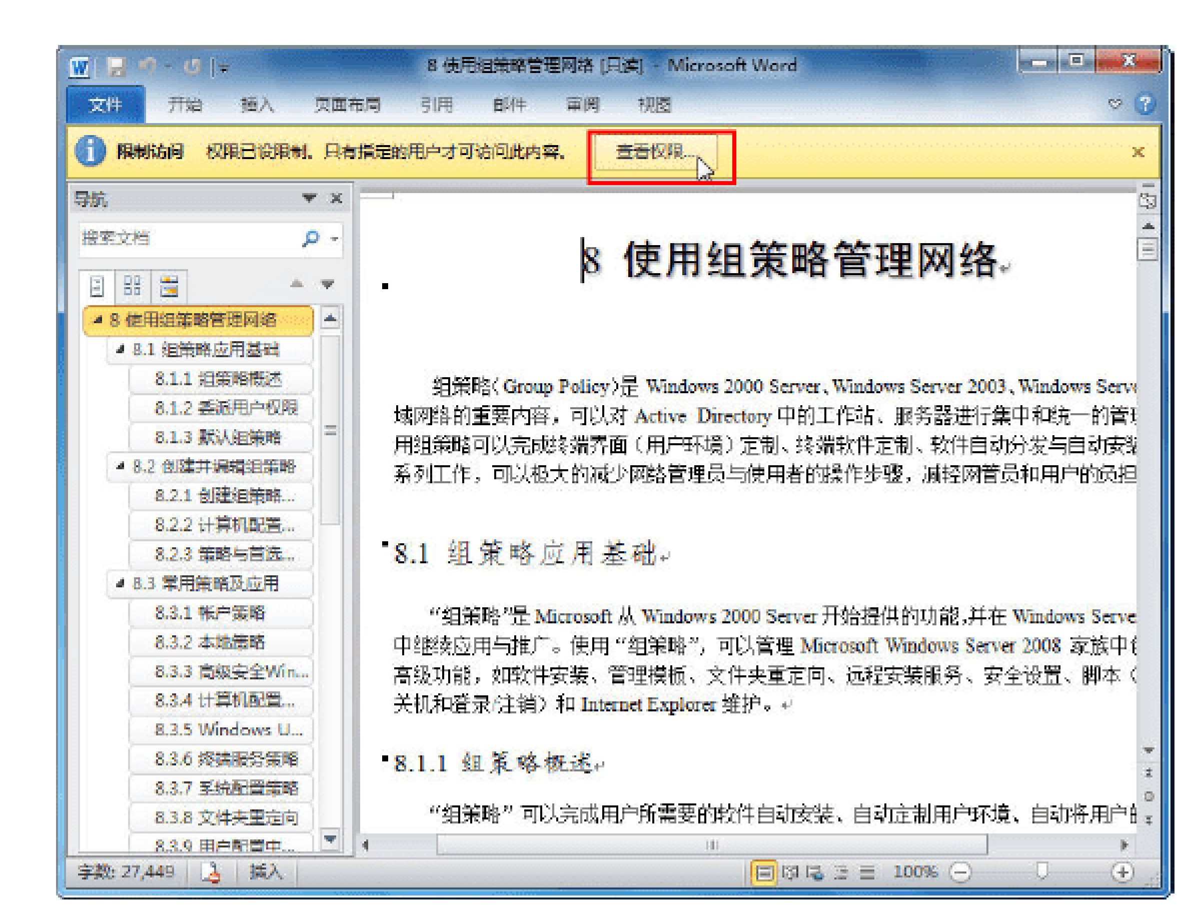


图 9-42　查看权限

如图 9-42 所示，“保存”按钮是“灰色”的，并且在该文档中不允许“复制”等操作。

05 在弹出的“我的权限”对话框中，显示了当前用户对该文档的权限，如图 9-43 所示。

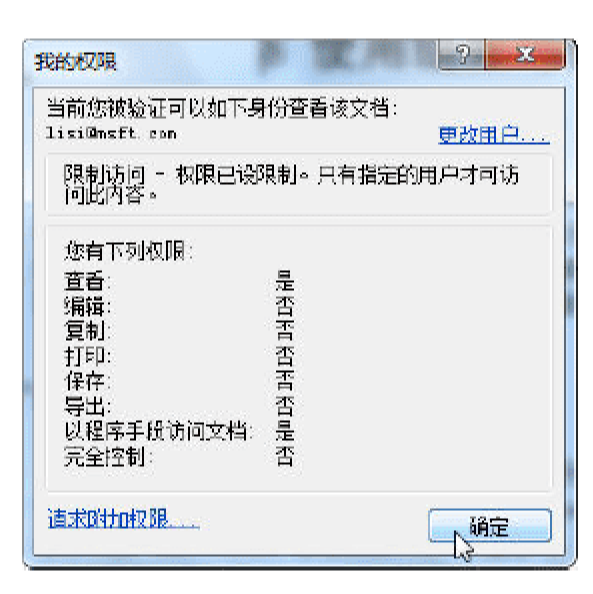


图 9-43　我的权限

9.4　在 Windows XP 客户端测试 RMS

如果 AD RMS 客户端运行在 Windows 2000 或 Windows XP SP1、SP2 系统，则必须安装客户端程序，否则在使用 Office 2003 的时候，如果选择“文件→权限→限制权限为”选项（如图 9-44 所示），则会弹出“Microsoft Office”的对话框，提示安装客户端程序，单击“是”按钮即开始下载 RMS 的客户端，如图 9-45 所示。

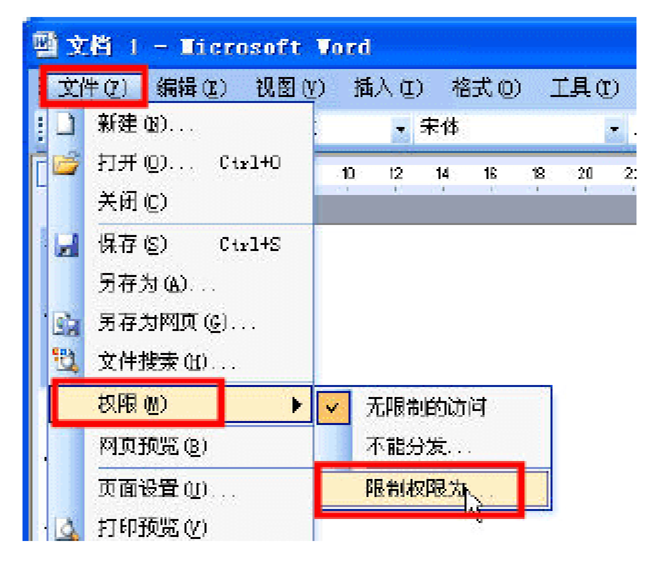


图 9-44　权限

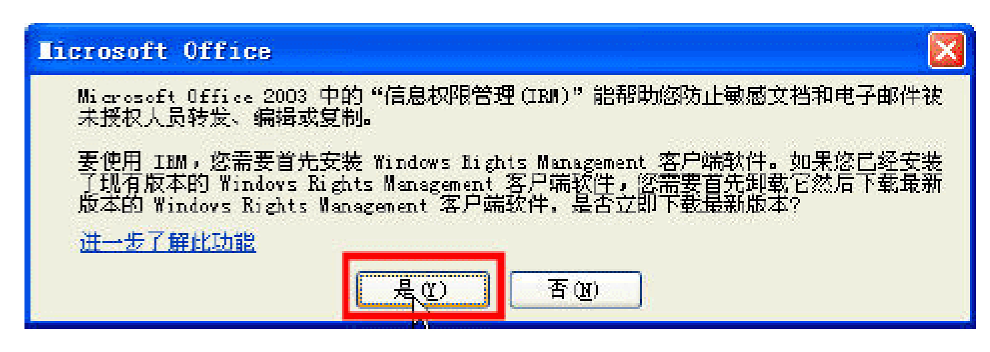


图 9-45　RMS 信息

用户也可以从 http://r.office.microsoft.com/r/rlidInstallDRMClient?clid=2052 下载 RMS 的客户端。RMS 客户端的安装比较简单，完全安装默认值即可完成安装，如图 9-46、图 9-47 所示。

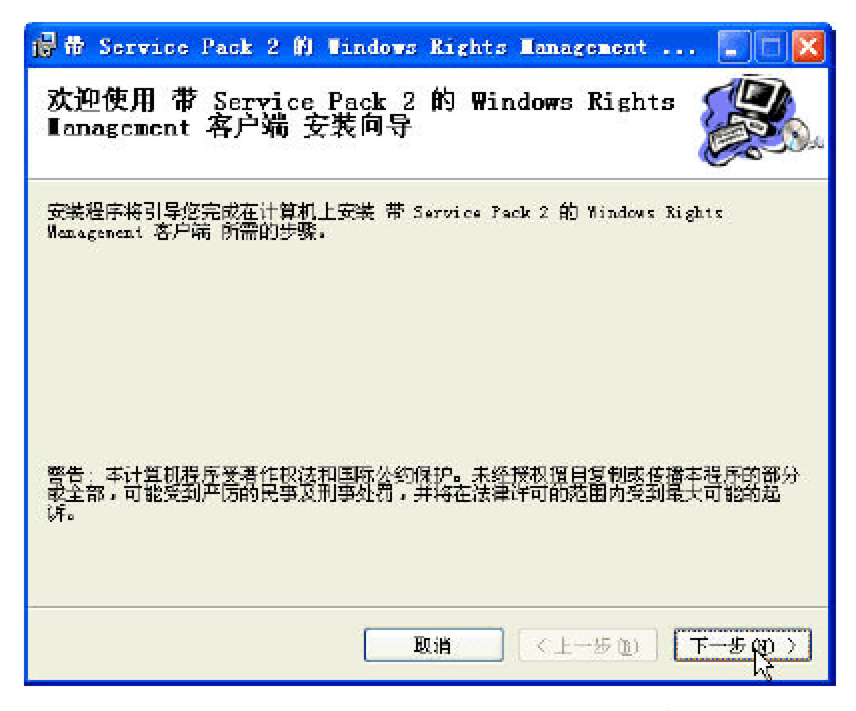


图 9-46　安装 RMS 客户端



图 9-47　安装完成

在安装了 RMS 客户端之后，就可以使用 RMS 服务器创建或打开受 RMS 保护的文档了。

但是，由于 Office 2003 使用的定义文件（用于启用 IRM 功能）中的许可证过期日期信息设置为 2009 年 12 月 10 日。所以，从 2009 年 12 月 11 日开始，使用 Office 2003 的客户将无法打开由 Active Directory Rights Management Service（AD RMS）或 Rights Management Services（RMS）保护的 Office 2003 文档。用户还需要从 http://support.microsoft.com/kb/978551/zh-cn 下载 office2003-KB978551-FullFile-ENU.exe，安装之后，才可以使用 RMS。该程序的安装也比较简单，完全按照默认值即可完成安装，如图 9-48、图 9-49 所示。

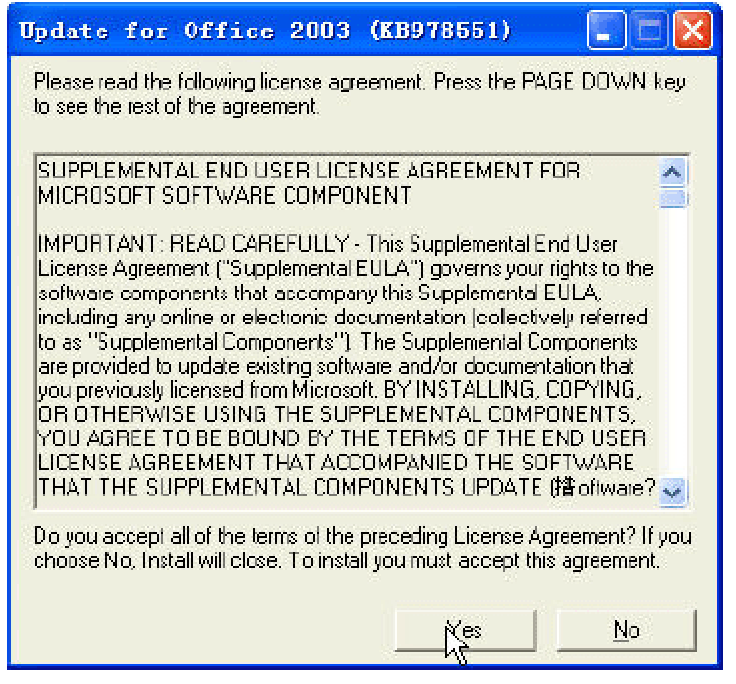


图 9-48　安装 KB978551 补丁



图 9-49　安装完成

9.4.1　在 Windows XP 中以张三身份登录

本小节将介绍使用 Office 2003 创建受 RMS 保护文档的操作，主要步骤如下。

01　以 rms1 的用户名登录，如图 9-50 所示。

02　打开 Word 2003，在“文档”菜单中选择“权限→限制权限为”选项，如图 9-51 所示。



图 9-50　以 rms1 登录

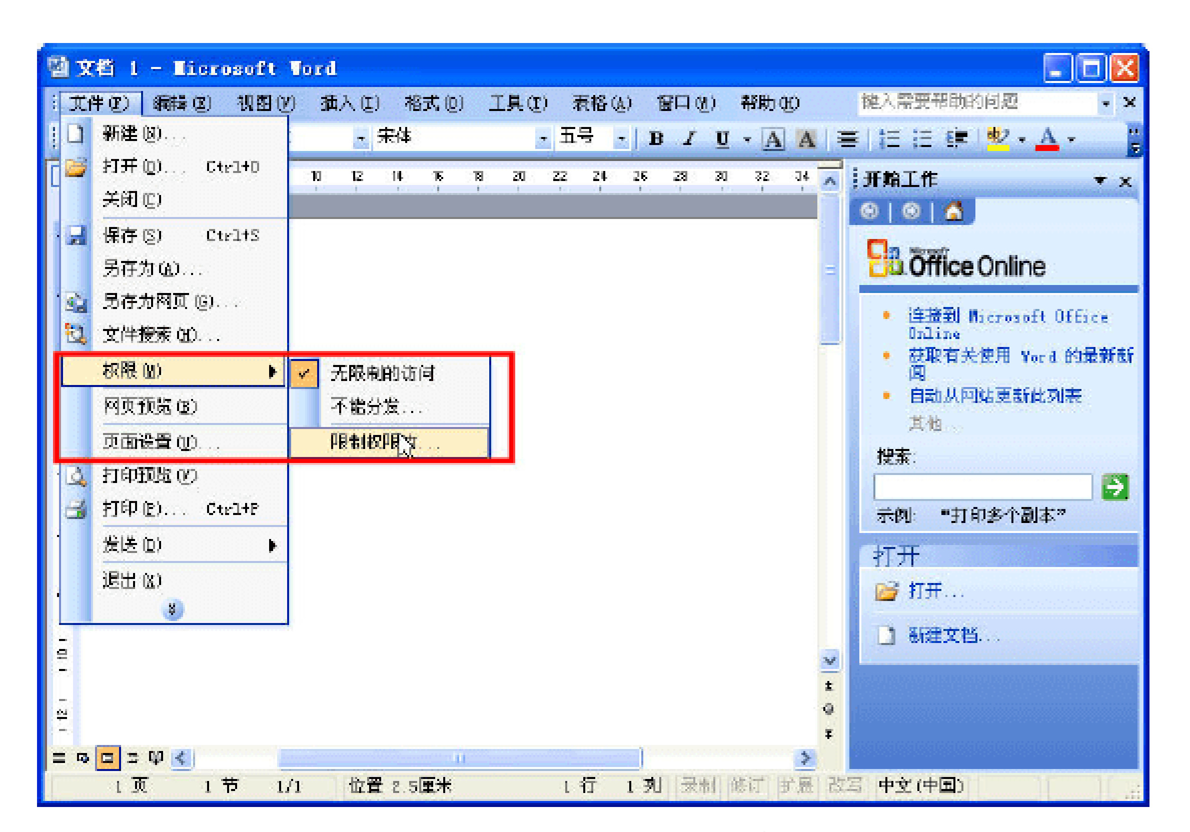


图 9-51　限制权限为

03 用域用户名 rms1 登录，并选中“记住我的密码”复选框，如图 9-52 所示。

04 在“选择用户”对话框中，选中“始终使用此账户”复选框，如图 9-53 所示。



图 9-52　记住我的密码



图 9-53　始终使用此账户

05 在“权限”对话框中，选中“限制对此文档的权限”复选框，并单击“其他选项”按钮，如图 9-54 所示。

06 在打开的“权限”对话框中，单击“确定”按钮，如图 9-55 所示。从“以下用户具有访问此文档的权限”列表中可以看到，只有当前用户才能访问该文档。

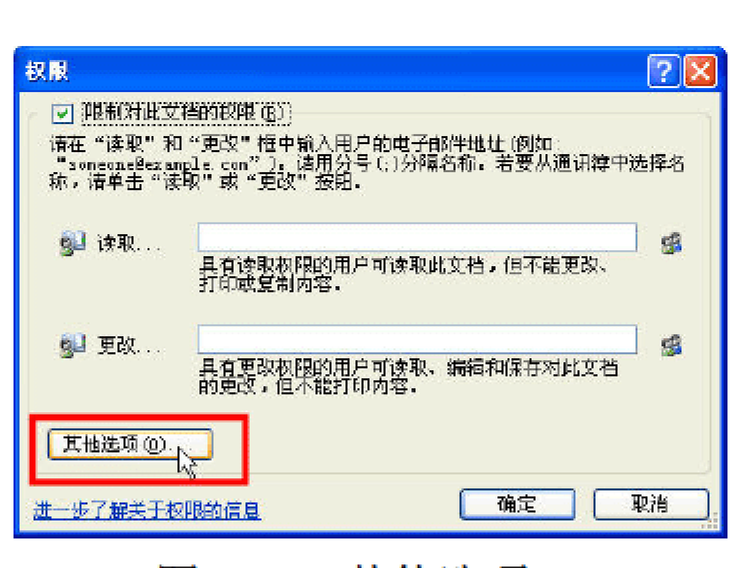


图 9-54　其他选项

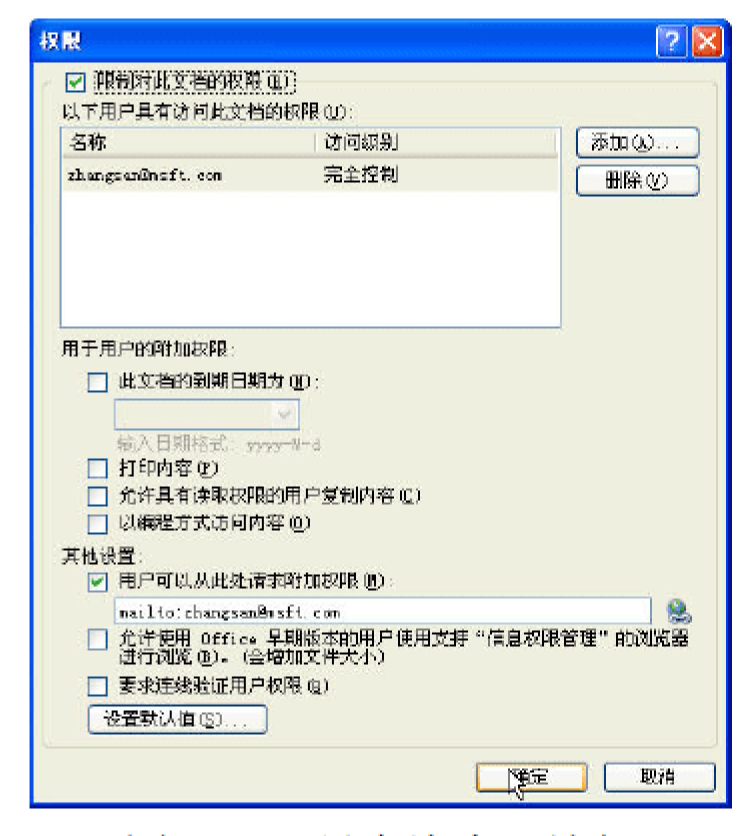


图 9-55　只允许自己访问

07 返回到编辑状态后，向文档中添加一些文字，如图 9-56 所示。然后将文档保存到 C 盘根

目录。

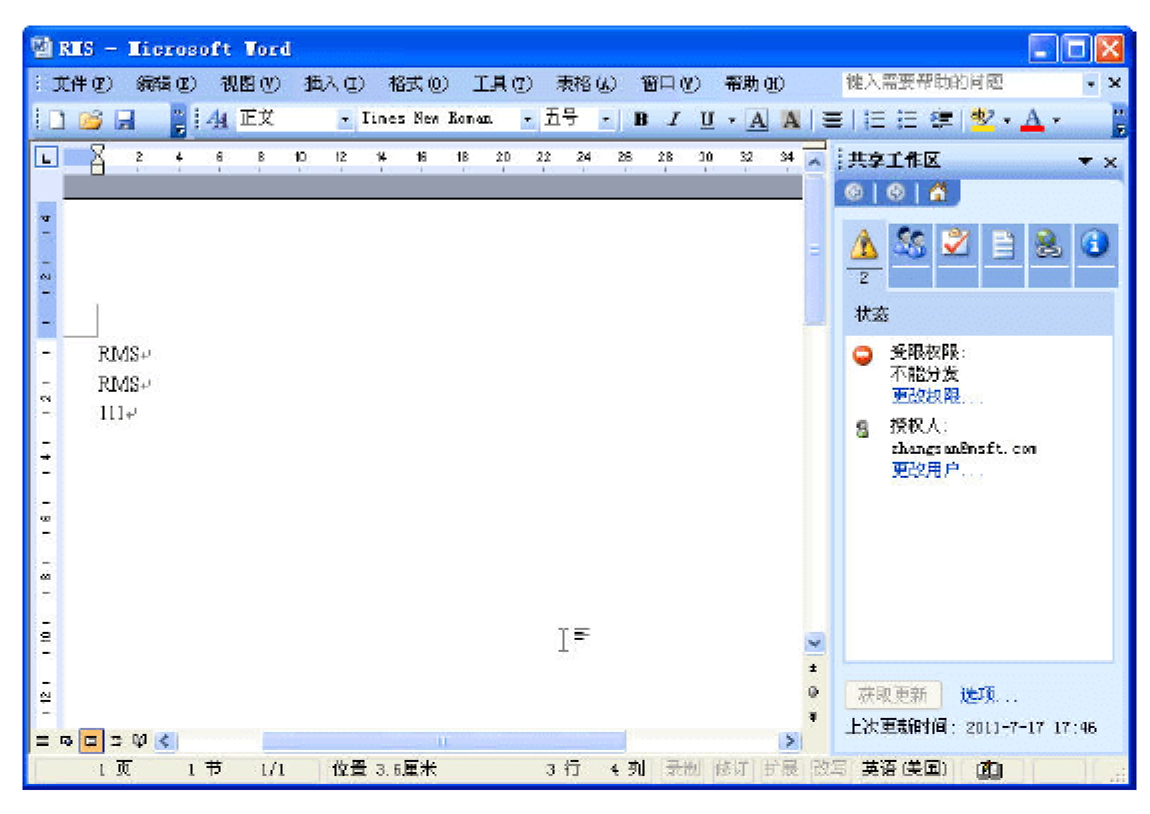


图 9-56 编写并保存文档

08 注销当前用户。

9.4.2 在 Windows XP 中以李四身份登录并查看文档

本小节以李四（rms2）身份登录，查看 9.4.1 小节（张三，rms1）保存的文档，主要步骤如下。

01 以 rms2 的用户名登录，如图 9-57 所示。

02 打开图 9-56 中保存的文档，首先会弹出“连接到 dc.heinfo.local”的对话框，输入用户名 rms2 及密码，如图 9-58 所示。



图 9-57 以 rms2 登录

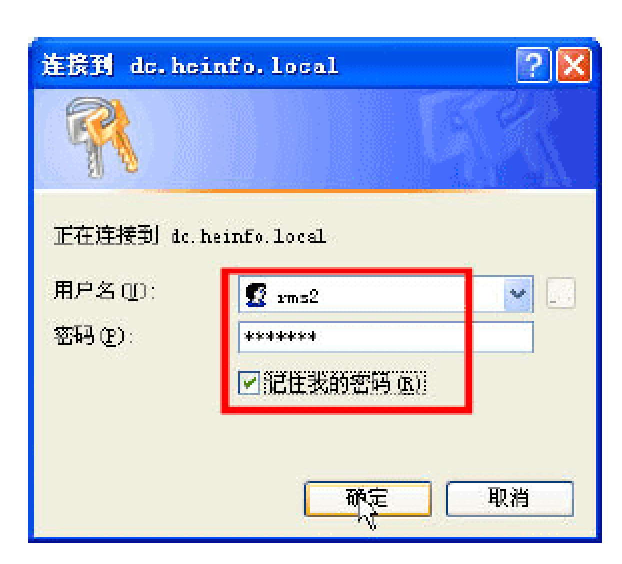


图 9-58 以李四身份登录

03 此时会弹出“您没有允许打开文档的凭据”对话框，如图 9-59 所示。



图 9-59 不能打开文档

04 如果尝试使用其他方式打开该文档（如图 9-60 所示），例如，通过“写字板”打开（如图 9-61 所示）。

05 用“写字板”打开 RMS 保护的文档后，只会显示“对此文档的权限当前受到限制”等信息，如图 9-62 所示。

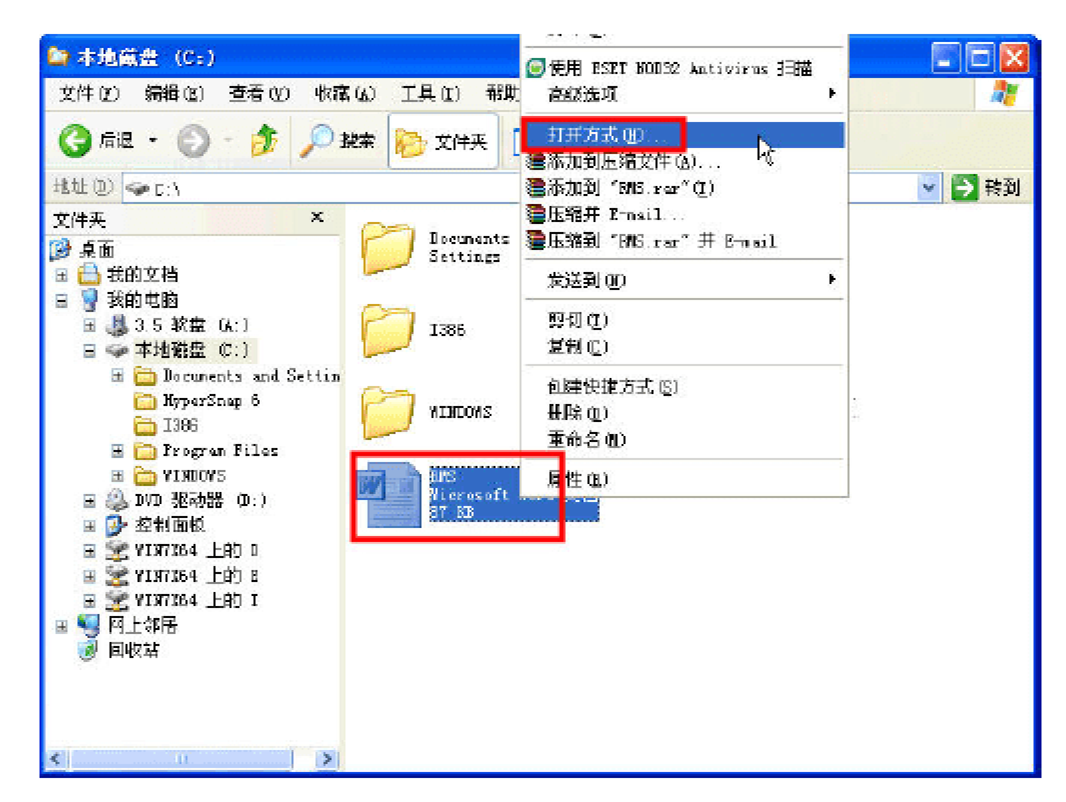



图 9-60　打开方式

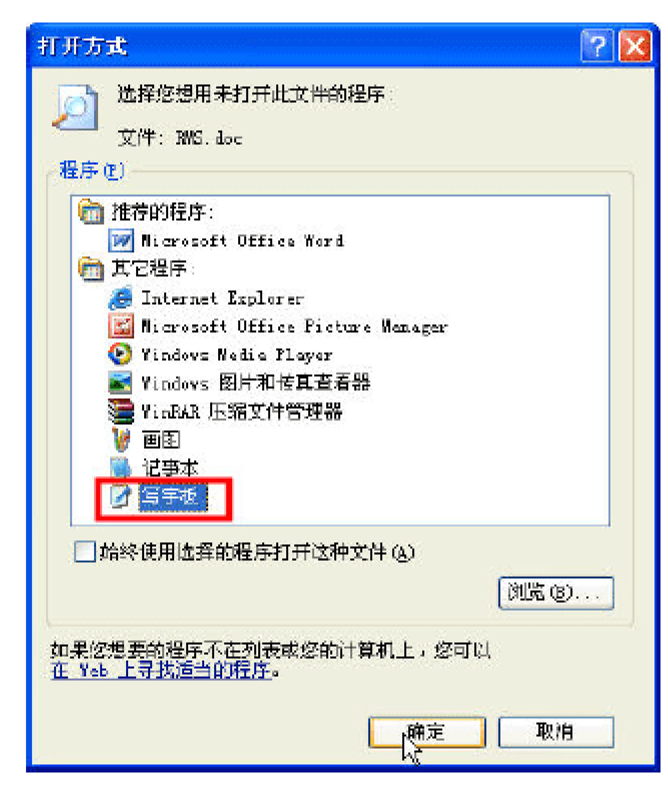


图 9-61　选择“写字板”

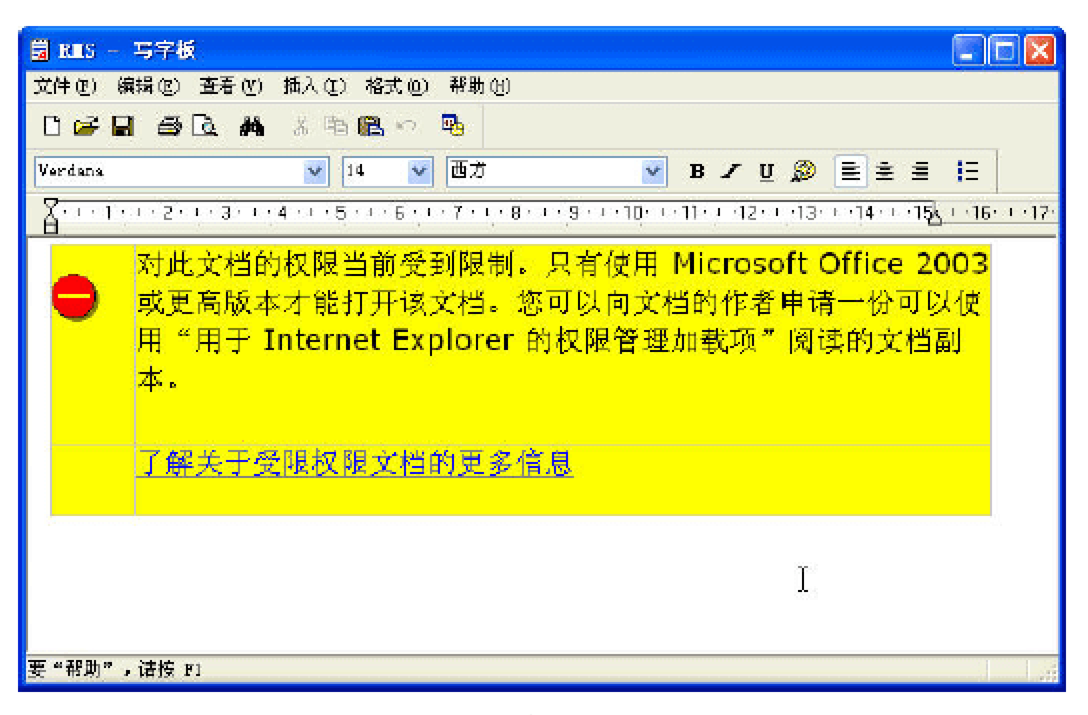


图 9-62　该文档权限受到限制

说 明

某些“电子签章”软件保护的 word 文档，使用 word 软件打开时，会出现其所控制的内容（不允许修改、查看等），但使用其他软件（例如图中的“写字板”）打开时，就会看到受保护的文档内容。目前，只有 RMS 保护的文档，才能达到管理员或单位主管所的安全要求，其他第三方软件都不能有效保护文档。

9.5　配置 AD RMS 服务器端

前面已经提到过，基本情况下，不需要对 AD RMS 服务器做进一步限制即可使用。但是，如果想要对 AD RMS 服务器端做进一步的了解，须从“开始→管理工具”中执行“Active Directory Rights Management Services”，打开 Active Directory Rights Management Services 管理单元，继续下面的内容。

9.5.1　配置信任策略

信任策略是不同 AD RMS 群集或不同域林中的 AD RMS 服务器之间建立信任关系的惟一标准，主要包括“受信任的用户域”和“受信任的发布域”。

1. 受信任的用户域

默认情况下，只有受信任的用户域才可以使用当前 AD RMS 服务器提供的权限保护服务，不同 AD RMS 群集或不同林中的 RMS 服务器都是通过彼此的许可证书识别的。用户可以通过将其他 AD RMS 群集中的信任用户域导出，并添加至本地服务器中，来实现对其他用户提供权限管理服务。导出的信任用户域文件中会包括原 AD RMS 服务器的许可证信息，因此建立信任关系后，来自该域的用户就可以使用当前 AD RMS 服务器提供的使用许可证。

01 在 AD RMS 控制台窗口中，定位到“信任策略→受信任的用户域”，如图 9-63 所示。在“受信任的用户域信息”列表中默认显示的是本地用户域，右击并选择快捷菜单中的“属性”选项即可查看其详细信息。

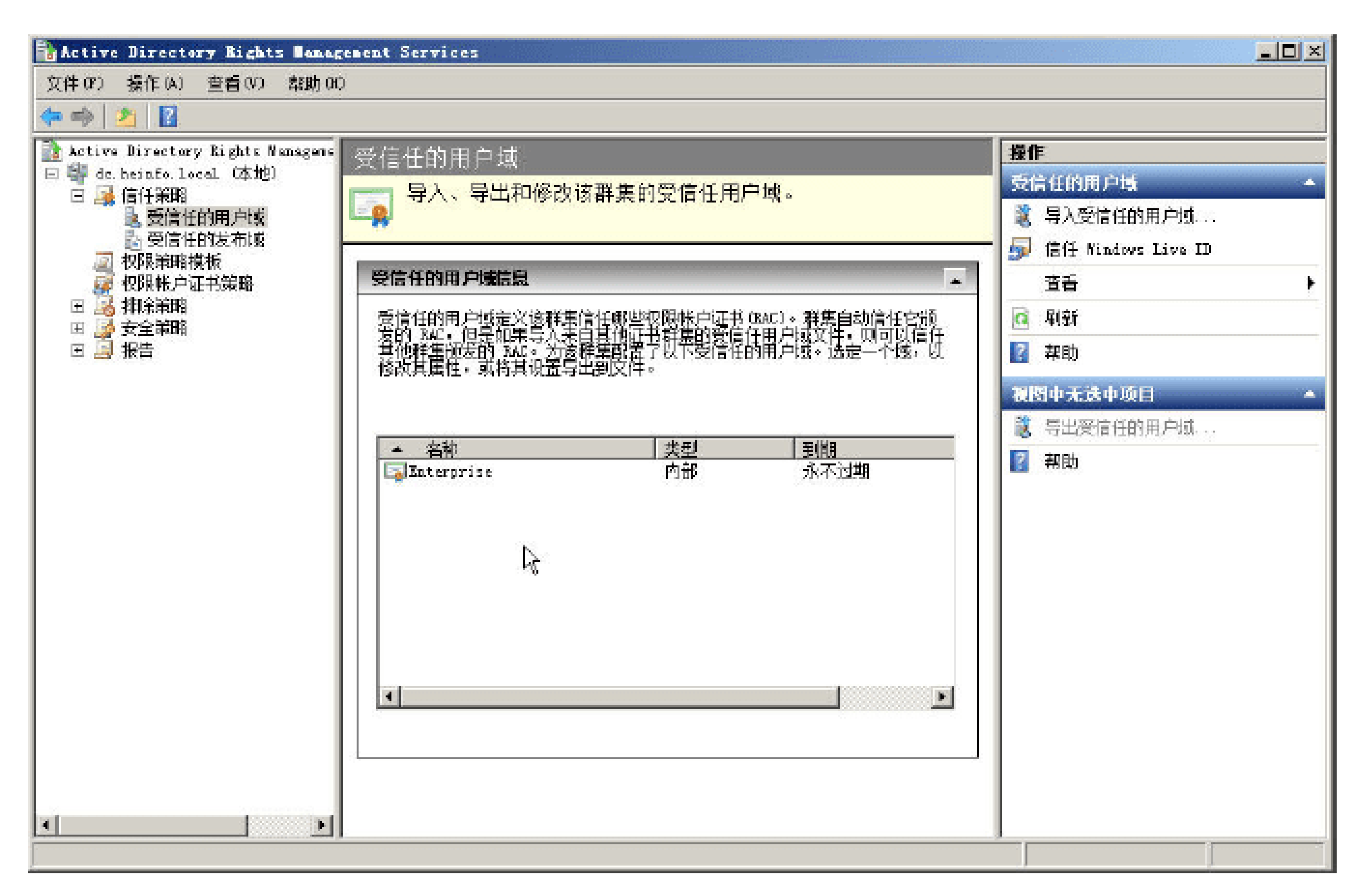


图 9-63　受信任的用户域

02 在图 9-63 右侧的“操作”栏中，单击“导入受信任的用户域”链接，显示如图 9-64 所示“导入受信任的用户域”对话框，在“受信任的用户域文件”文本框中输入文件的保存路径，或单击“浏览”按钮进行选择；在“显示名称”文本框中，输入该用户将在列表中显示的名称，用来进行标识。

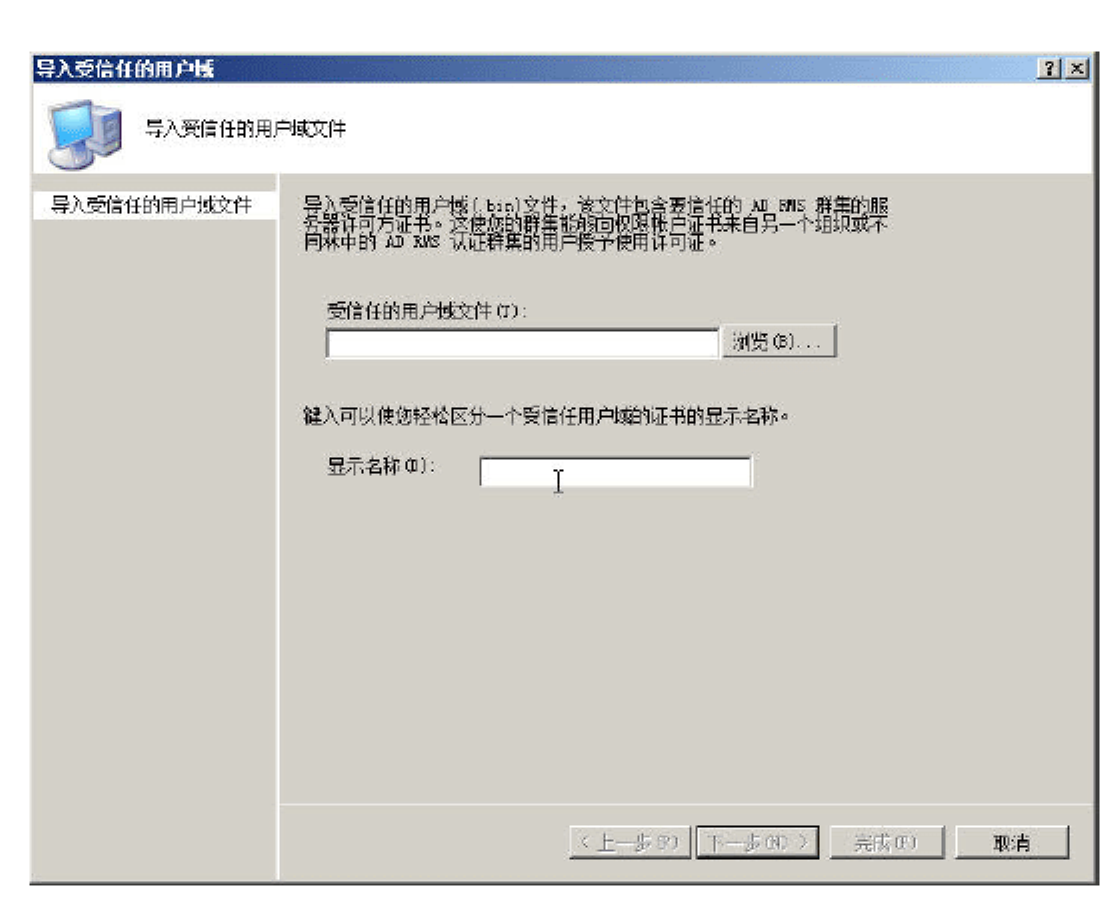
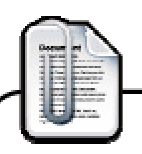


图 9-64　导入受信任的用户域

03 单击“完成”按钮，即可完成用户域的添加。重复操作，可添加多个受信任的用户域。



提 示

在“受信任的用户域信息”列表中，右击用户域并选择快捷菜单中的“导出受信任的用户域”选项，还可以将其导出，以备本地恢复使用；也可以导入到其他 AD RMS 群集中，用于接受其他 AD RMS 服务器的权限许可证。

2. 受信任的发布域

在 AD RMS 控制台窗口中，单击“受信任的发布域”选项将显示如图 9-65 所示“受信任的发布域信息”窗口。

受信任的发布域用于定义哪些 AD RMS 群集发布的许可证可以受到此群集的信任，与受信任的用户域恰恰相反，列表中默认存在的是本地服务器的记录。受信任的发布域文件的导出和导入与受信任的用户域文件类似，不同的是发布域文件的类型为.XML，其中包括将要信任的 AD RMS 服务器许可方证书、群集密钥和模板等信息。另外，发布域文件本身是受密码保护的，导入时必须输入原 AD RMS 服务器上使用的存储密码。

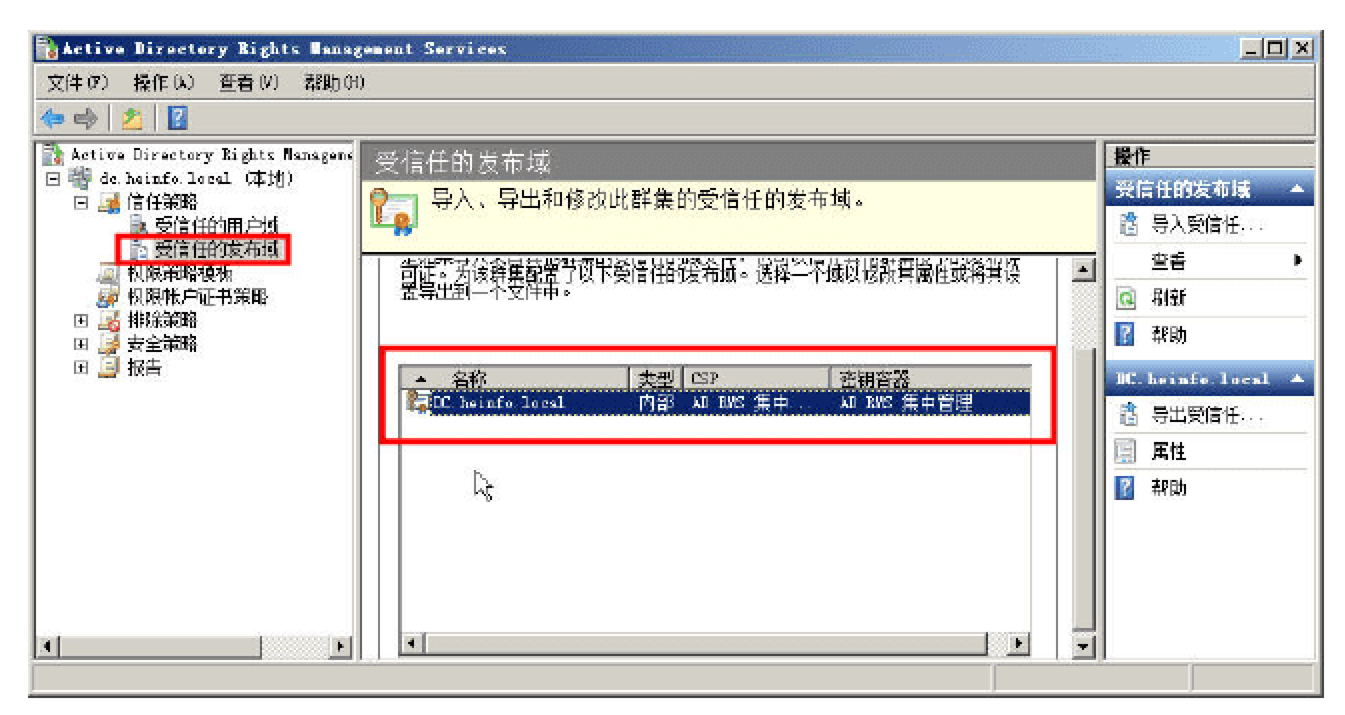


图 9-65　受信任的发布域

9.5.2　配置权限策略模板

使用 Active Directory Rights Management Services 控制台，可配置权限策略模板。配置权限策略模板后，这些模板将存储在配置数据库和可选的共享文件夹中。权限策略模板用于控制用户或组对受权限保护的特定内容所具有的权限。AD RMS 在配置数据库中存储权限策略模板，或者，在用户指定的共享文件夹中保留所有权限策略模板的副本。

1. 创建权限策略模板

机密程度不同的文档发布到客户端后设置的权限也有所不同，此时就需要为该文档应用不同级别权限的策略模板。权限策略模板是为定义用户的权限策略准备的，管理员可以通过定制一些现成的策略模板让企业用户直接调用。

01 在“AD RMS 控制台”窗口中，单击“权限策略模板”选项，显示如图 9-66 所示“分布式权限策略模板”窗口。

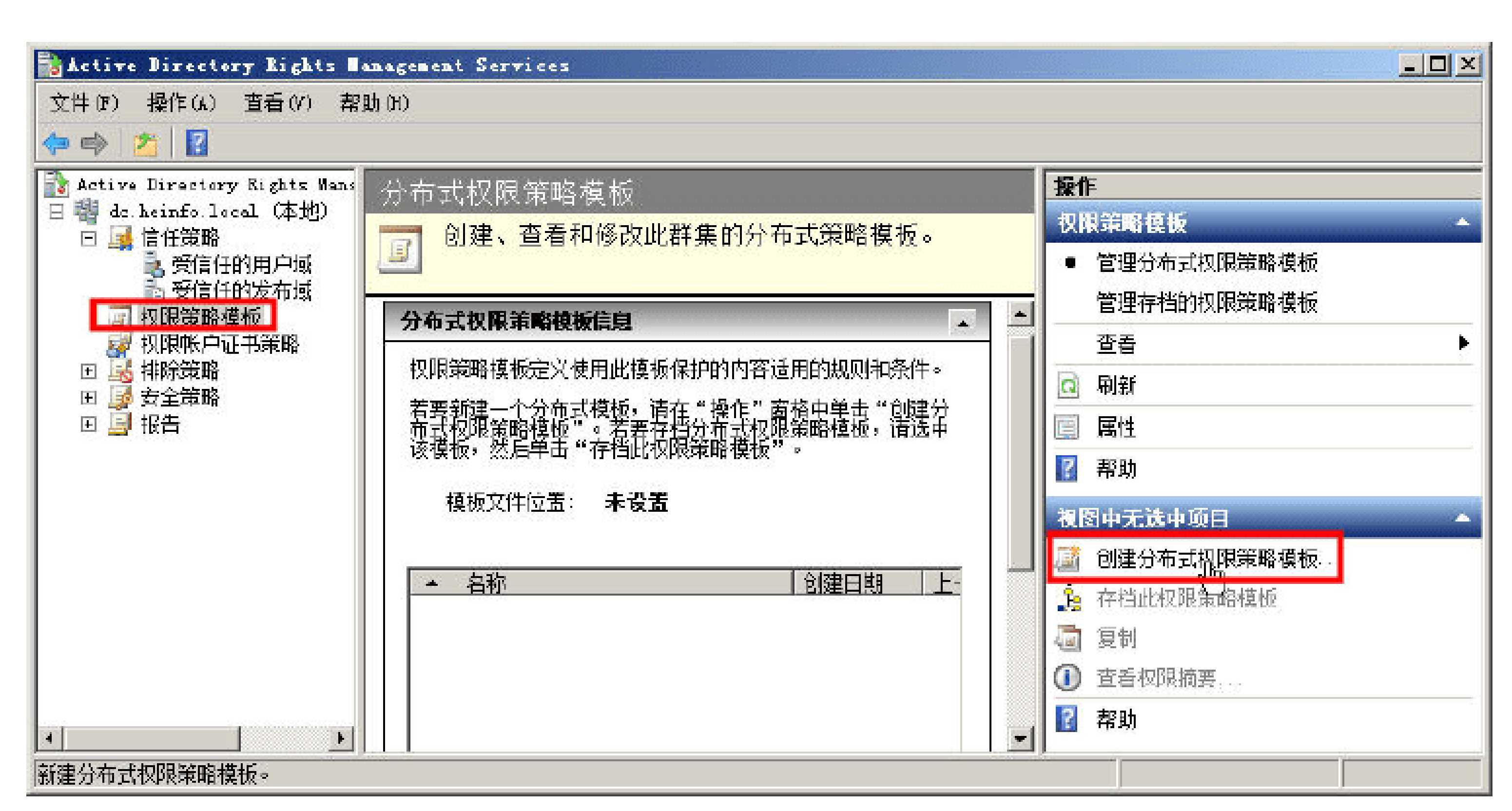


图 9-66 分布式权限策略模板

02 单击图 9-66 右侧“操作”栏中的“创建分布式权限策略模板”链接，启动创建向导，首先显示如图 9-67 所示的“添加模板标识信息”对话框。

03 单击“添加”按钮，显示如图 9-68 所示“添加新的模板标识信息”对话框。在“语言”下拉列表中选择客户端所使用的语言，在“名称”文本框中输入新建模板的名称，单击“添加”按钮，将其添加至“模板标识”列表中。

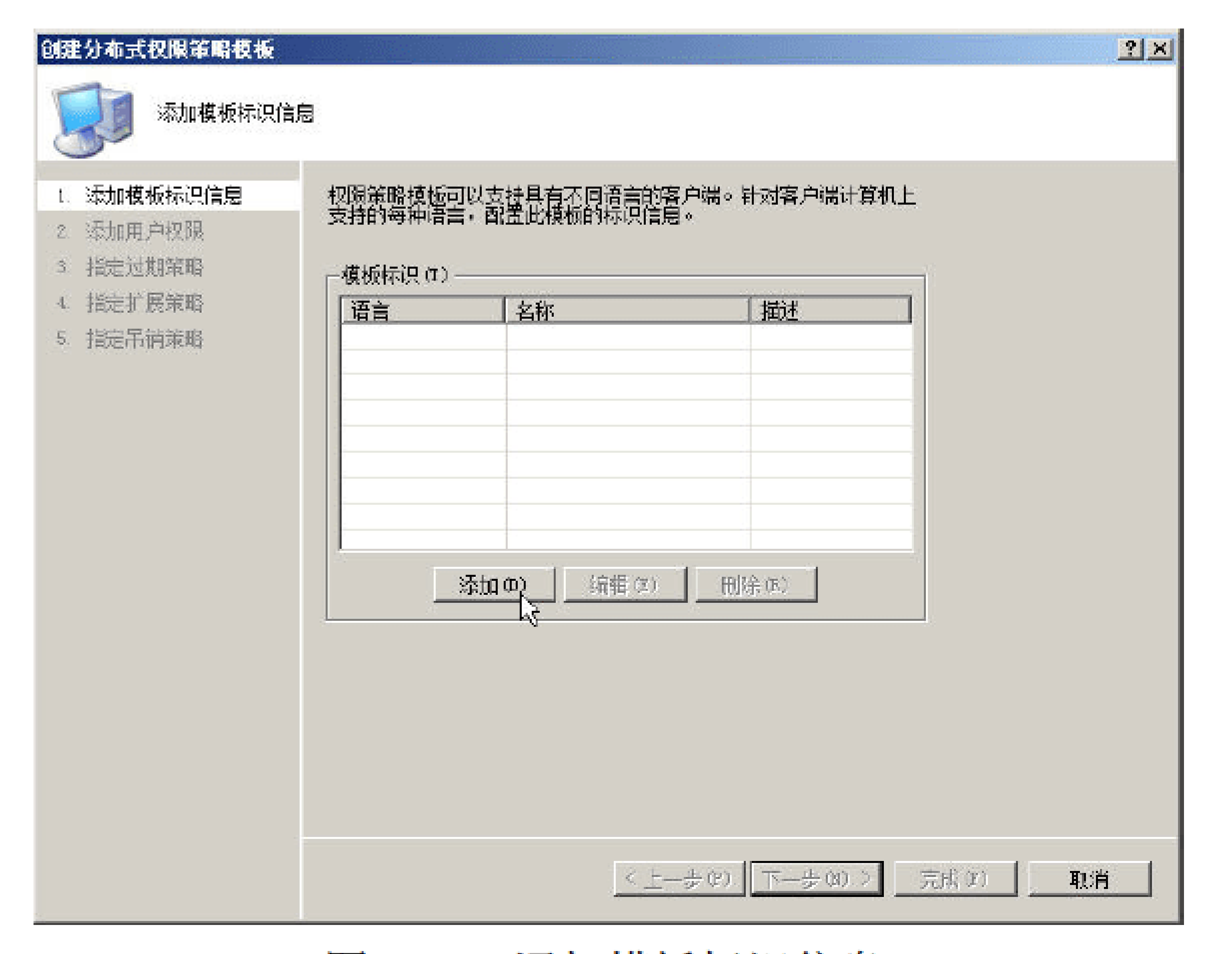


图 9-67 添加模板标识信息

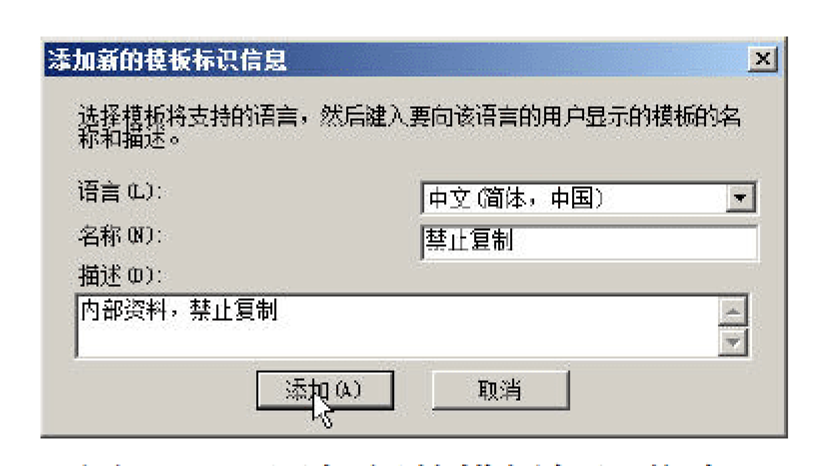


图 9-68 添加新的模板标识信息

04 单击“下一步”按钮，显示如图 9-69 所示“添加用户权限”对话框，默认情况下“用户和权限”列表是空的，即只“授予所有者不会过期的完全控制权限”，其他用户账户没有任何权限。

05 单击“添加”按钮，显示如图 9-70 所示“添加用户或组”对话框。选择“用户或组的电子邮件地址”单选按钮，即可在下面的文本框中输入用户对应的电子邮件地址，或者单击“浏览”按钮从域中查找添加。如果选择“任何人”单选按钮，则对当前域中的所有用户账户有效。

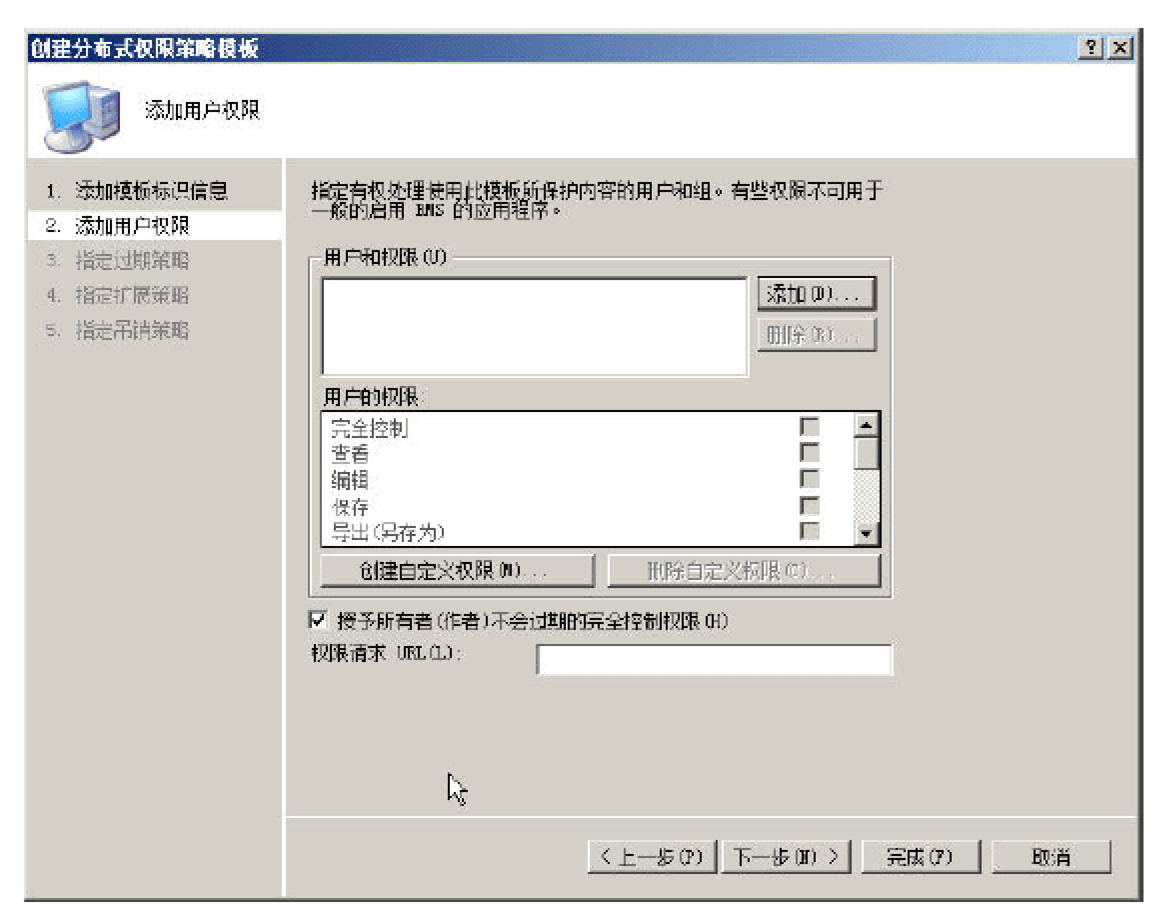


图 9-69　添加用户权限

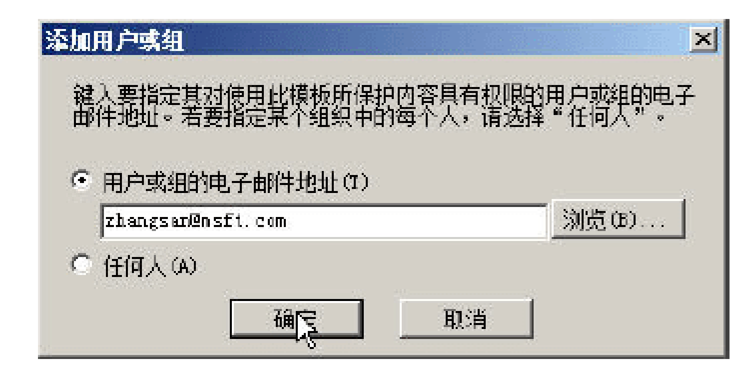


图 9-70　添加用户或组



说 明

如果要添加用户，应事先在域控制器上，打开用户属性对话框，为用户添加电子邮件地址，如图 9-71 所示。同样，如果要添加用户组，也要打开用户组属性，添加电子邮件地址，如图 9-72 所示。

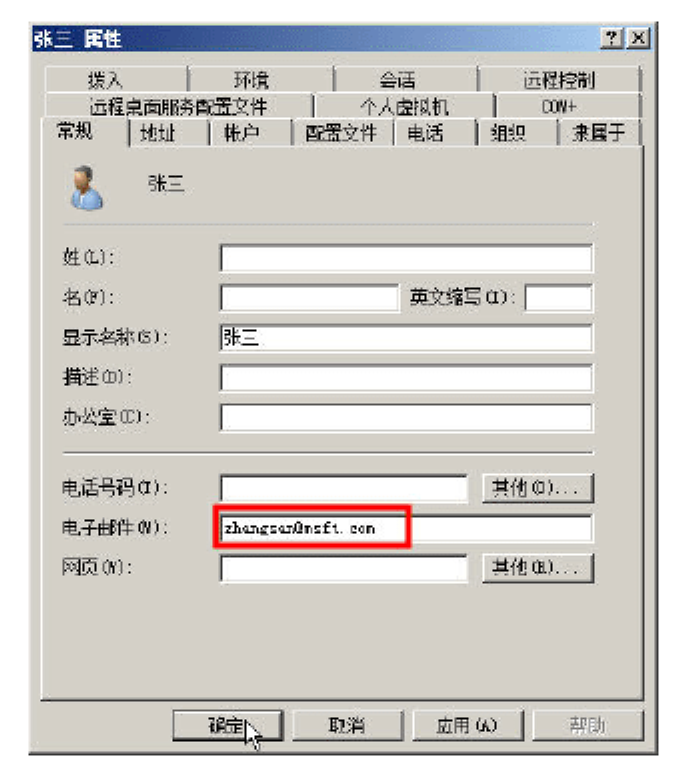


图 9-71　添加用户电子邮件地址

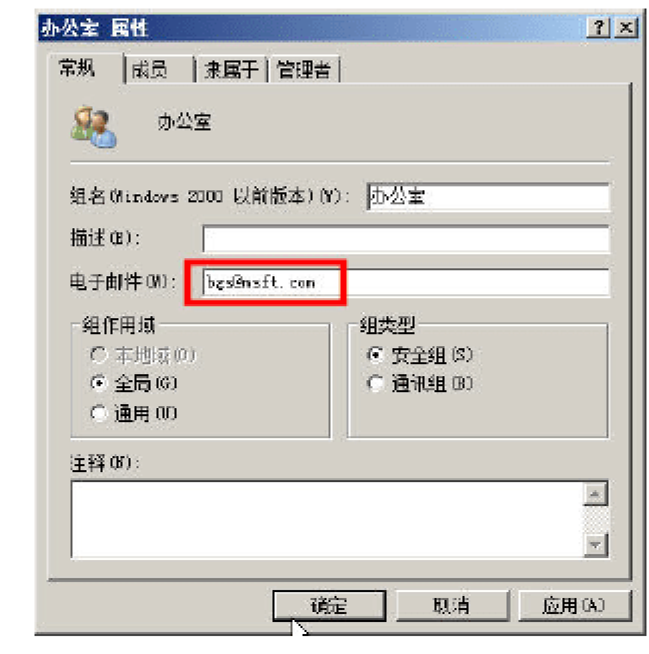
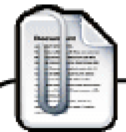


图 9-72　添加用户组电子邮件地址

06 单击“确定”按钮，将所选用户添加至列表中，如图 9-73 所示。重复操作，可添加多个用户或组的电子邮件地址。然后，在“用户和权限”列表中，选择赋予用户的权限，例如，要求做到“禁止复制”，则只选择“查看权限”复选框即可。

07 单击“下一步”按钮，显示如图 9-74 所示的“指定过期策略”对话框。在“内容有效期限”选项区域中，可以定义当前模板中的权限信息何时过期或有效期限等，默认为“永不过期”。内容过期后，如果仍需要使用该策略信息，则必须重新发布一次。



说 明

“权限请求 URL”是当模板赋予用户的权限无法完成相应工作，或在模板权限规定的时间和日期内没有完成工作时，用户可以通过此 URL 继续向管理员发出权限请求，以再次获得权限或附加权限。权限列表中给出的所有权限都是允许的，即只要选择某项，就表示要赋予用户具有相应的权限。

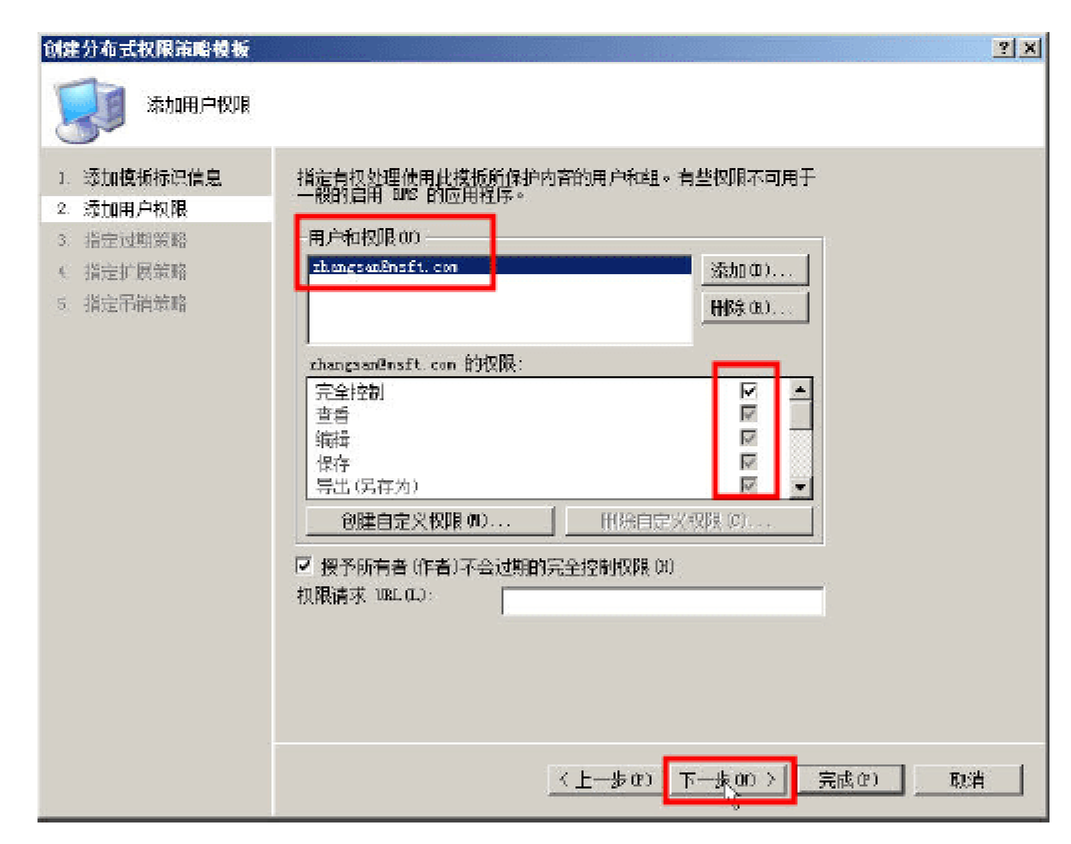


图 9-73　指定用户权限



图 9-74　指定过期策略

08 单击“下一步”按钮，显示如图 9-75 所示的“指定扩展策略”对话框。在“使用此模板指定受保护内容的其他条件”选项组中有 3 个选项，如下所示：

- “使用户能够使用浏览器加载项查看受保护的内容”：该项对于没有安装 Office 的客户端是非常实用的，只须安装相关插件即可在浏览器中查看受 RMS 保护的 Office 文档，建议选择该项。
- “每次使用内容时需要更新使用许可证（禁用客户端缓存）”：该项虽然可以使被保护文档更安全，但客户端每次使用时会非常繁琐。
- “如果您要为启用 AD RMS 的应用程序指定其他信息，则可以在此处以名称-值对的形式指定”：选中该复选框，可在下面的列表中添加特定应用程序需要的名称和权限值，普通用户无须设置。

09 单击“下一步”按钮，显示如图 9-76 所示“指定吊销策略”对话框。吊销是 AD RMS 的一项重要功能，实施吊销之前必须先手动创建一个吊销列表，并为每个吊销列表生成一个公钥/私钥对，然后使用私钥签署吊销列表；另外，还必须为吊销列表指定一个用户可以访问的 URL 地址或 UNC 路径。通常情况下，不需要 AD RMS 服务器吊销，即不选择该复选框。





图 9-75　“指定扩展策略”对话框

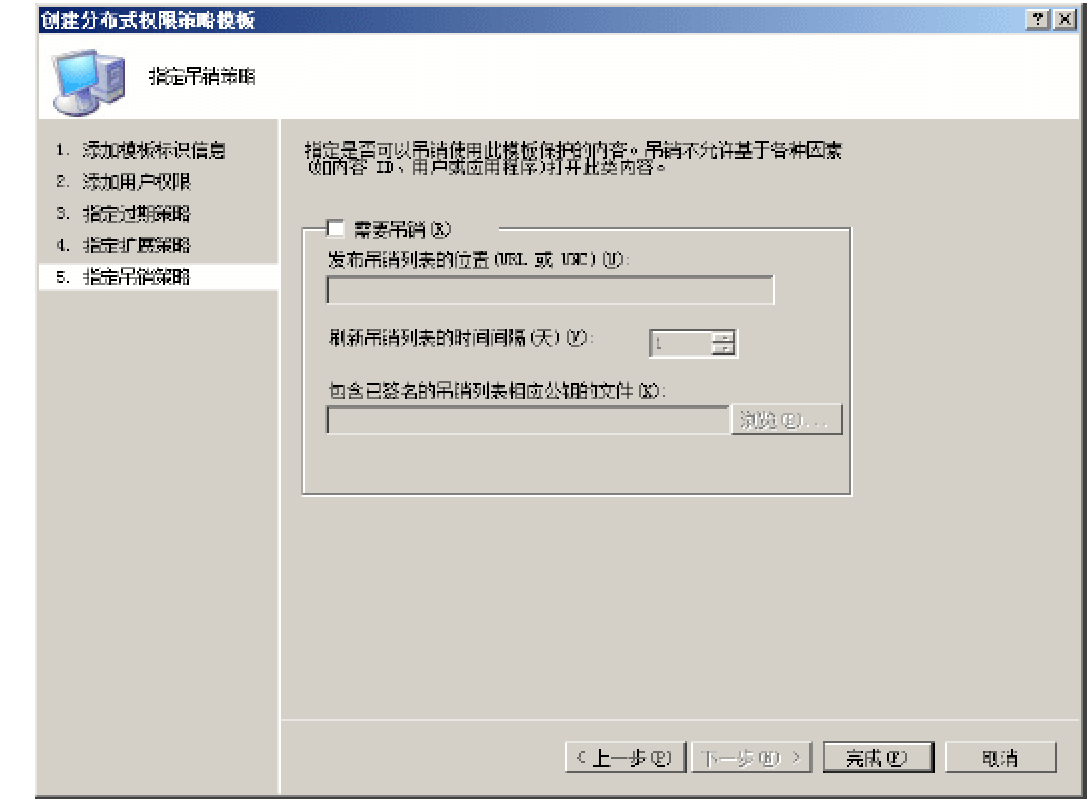


图 9-76　“指定吊销策略”对话框

10 单击“完成”按钮，退出创建向导，返回“权限策略模板”窗口，如图 9-77 所示。新创

建的模板已经出现在列表中，此时虽然已经创建成功，但并不能立即应用。

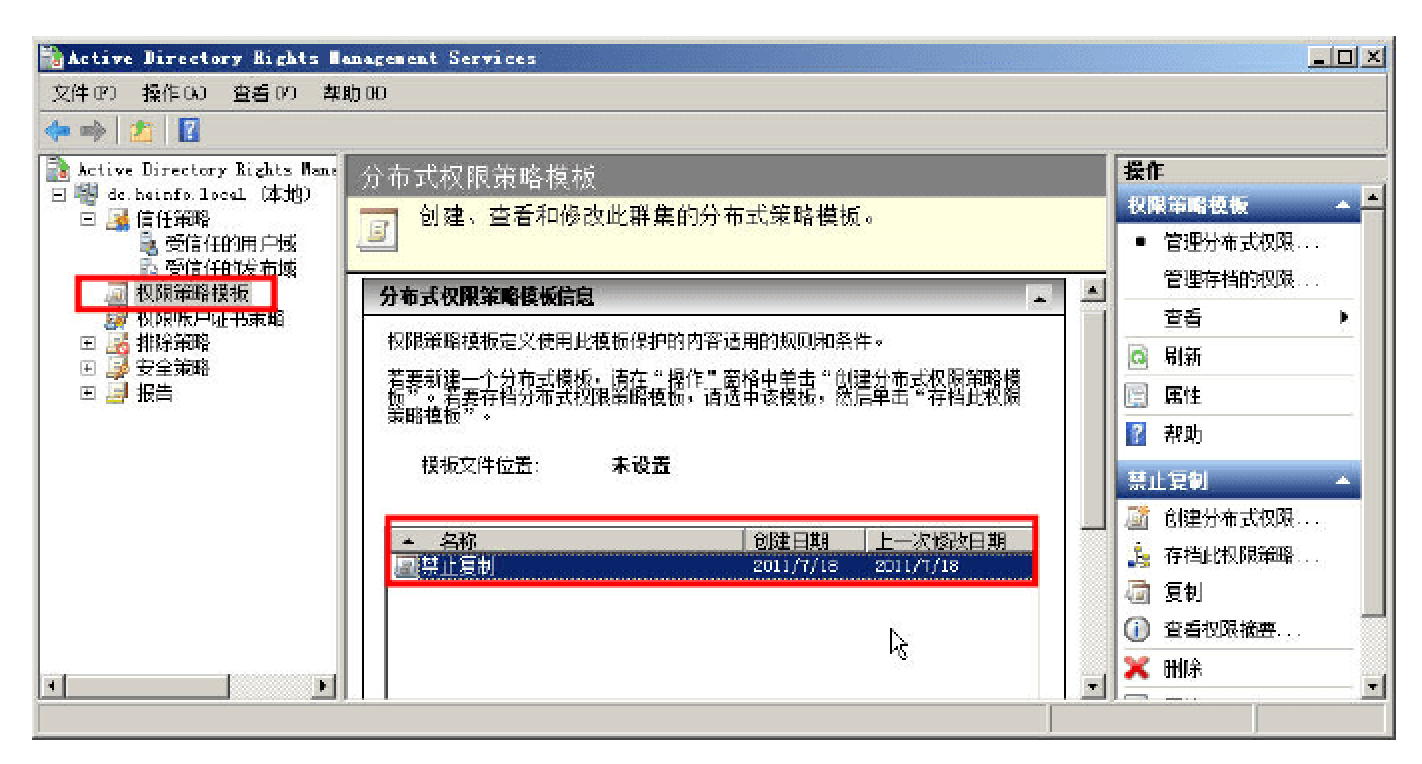


图 9-77　权限策略模板创建成功

11 选择新创建的策略模板，右击并选择快捷菜单中的“存档此分布式权限策略模板”选项，将其本地存档，显示如图 9-78 所示提示框，提示一旦保存后，将不能再分发或导出该模板。

12 单击“是”按钮保存，新创建的权限策略模板保存到本地模板库中备用。返回“分布式权限策略模板”窗口，单击“管理存档的权限策略模板”链接，所有已存档的策略模板即可显示在“公布式权限策略模板”列表框中，管理员可以继续修改和查看其各项属性信息。如图 9-79 所示是新建策略模板的权限摘要。

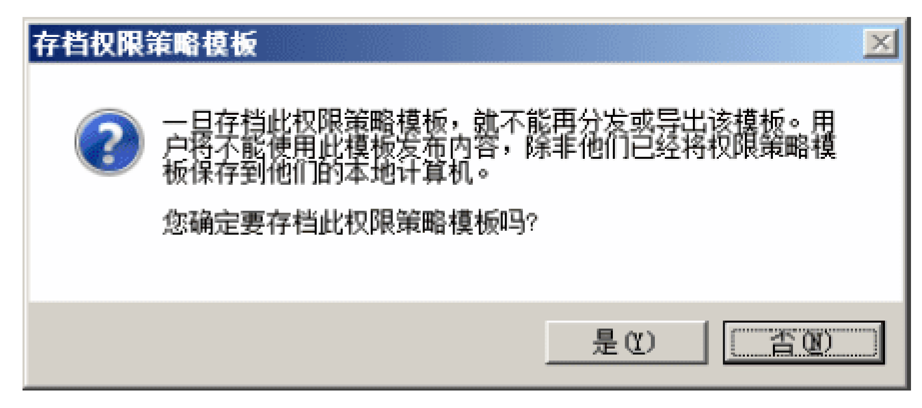


图 9-78　存档权限策略模板

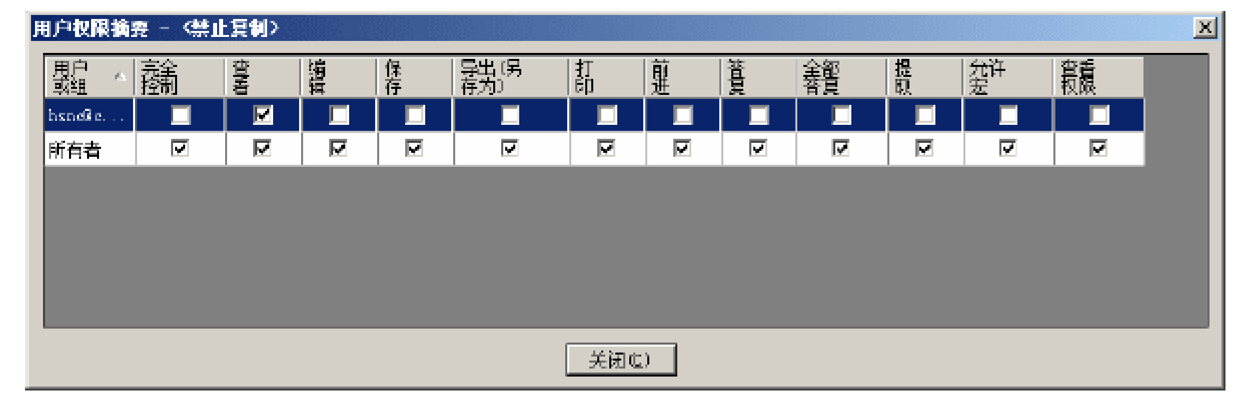


图 9-79　用户权限摘要

2. 分发权限策略模板

客户端必须将服务器上创建的权限策略模板保存到本地计算机才可以使用，可以通过文件共享、网络传输、移动存储介质等方式获得。默认情况下，权限策略模板的保存位置为“未设置”。为了便于保存和用户使用，应在群集中指定一个公共文件夹，用于保存所有的策略模板。

01 在“权限策略模板”窗口中，单击“操作”栏中的“管理分布式策略模板”链接，然后单击“属性”链接，打开如图 9-80 所示“权限策略模板 属性”对话框。

02 选择“启用导出”复选框，在“指定模板文件位置”文本框中输入已经设置好的共享文件夹路径，如图 9-81 所示。注意，这里必须使用 UNC 格式，并且确定已经为指定用户账户赋予了写入权限。

03 设置完成后单击“确定”按钮。然后，单击“管理存档权限策略模板”链接，选择想要分发的模板，右击并选择快捷菜

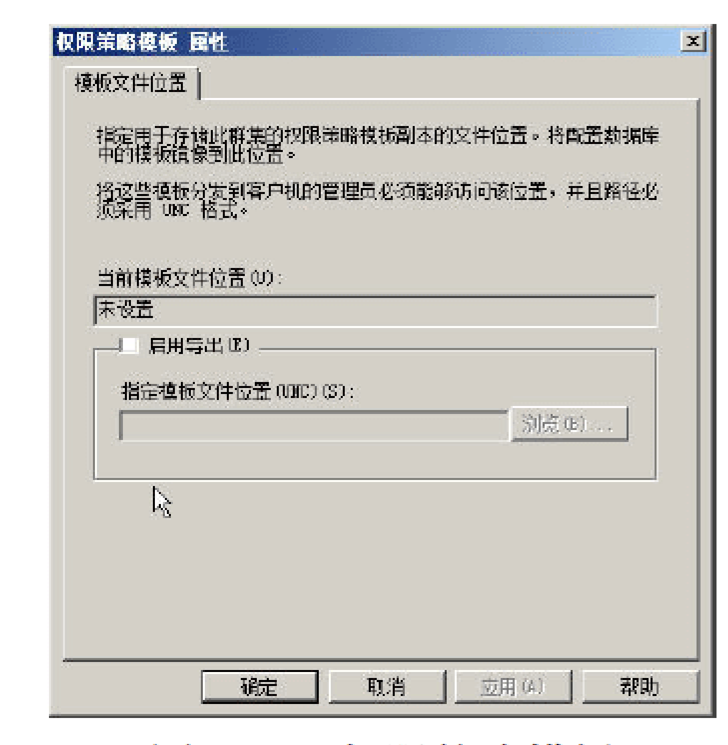


图 9-80　权限策略模板

单中的“分发此权限策略模板”选项，显示如图 9-82 所示“分发权限策略模板”对话框。提示分发之后，用户便可以使用此模板发布新内容。

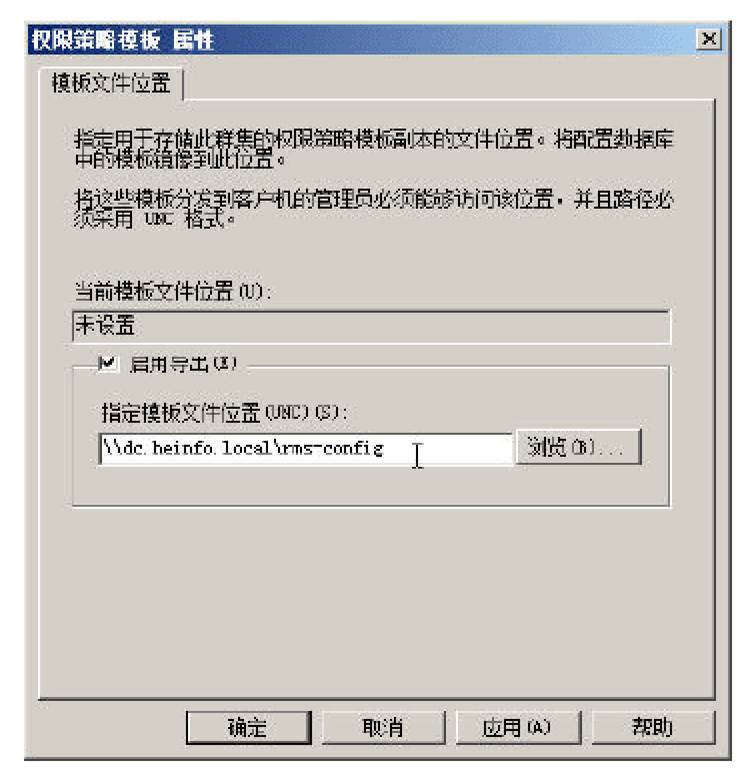


图 9-81　设置共享文件夹路径

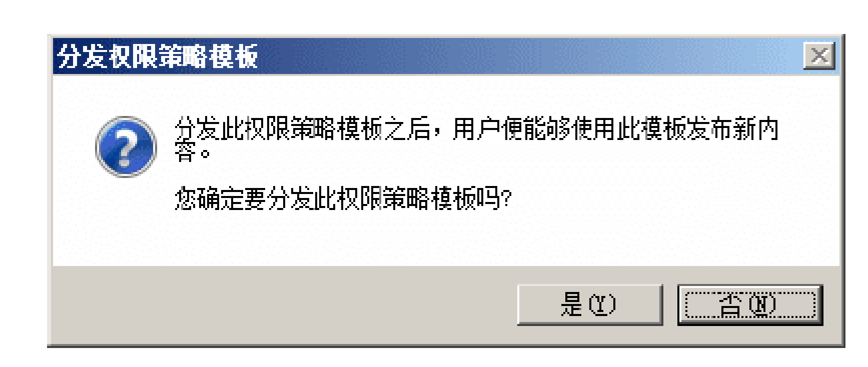


图 9-82　分发权限策略模板

04 单击“是”按钮确认即可。



说 明

如果模板是从另一台 RMS 服务器迁移到此 RMS 服务器上的，在使用该模板之前，必须由此服务器签署，然后重新分发到客户端。

3. 撤销权限策略模板

当某个权限策略模板不再适用时，可以将其删除。删除权限策略模板时，同时应删除用户计算机上的该模板，以便用户试图使用已撤销的权限策略模板发布内容时不会出现问题。当用户使用权限策略模板发布内容时，该发布请求将被发送到 RMS 服务器。RMS 将使用数据库中存储的该权限策略模板的副本来响应该请求。如果数据库中不存在该权限策略模板，请求将失败。

4. 备份和恢复权限策略模板

要保护重要的权限策略模板，可以将配置数据库中的模板数据定期备份到媒体中，并将该媒体存放到安全的地方。这样，当系统发生故障时，管理员就可以使用备份的副本来恢复权限策略模板。

9.5.3　配置权限账户证书策略

权限账户证书（RAC）是 AD RMS 服务器颁发给每个客户的认证凭证，该证书将用户账户与一个受保护的密钥对关联，而密钥对则专用于用户的计算机。用户可以通过这些证书来发布和使用受 AD RMS 保护的内容。每个证书都包含一个公钥，以向用户授予使用相关信息的权限。

01 在“AD RMS 控制台”窗口中，在左侧栏中单击“权限账户证书策略”选项，显示如图 9-83 所示“权限账户证书策略”窗口。权限账户证书根据有效期的长短和应用环境的不同，可分为标准 RAC 和临时 RAC。标准 RAC 的默认有效期限是 365 天，通常应用于固定用户的计算机上；临时 RAC 的默认有效期限为 15 分钟，主要是为了方便用户在不同位置都可以使用受 AD RMS 保护的文档。

图 9-83　权限账户证书策略

02 权限账户证书的有效期限可以根据实际需要更改。单击“更改标准 RAC 有效期”链接，显示如图 9-84 所示“权限账户证书策略”对话框，在“标准 RAC 的有效期（天）”文本框中输入合适数值即可，有效期的范围是 1~9 999 天。

03 选择“临时 RAC”选项卡，或者在“权限账户证书策略”窗口中单击“更改临时 RAC 有效期”链接，也可以更改临时 RAC 的有效期，如图 9-85 所示。

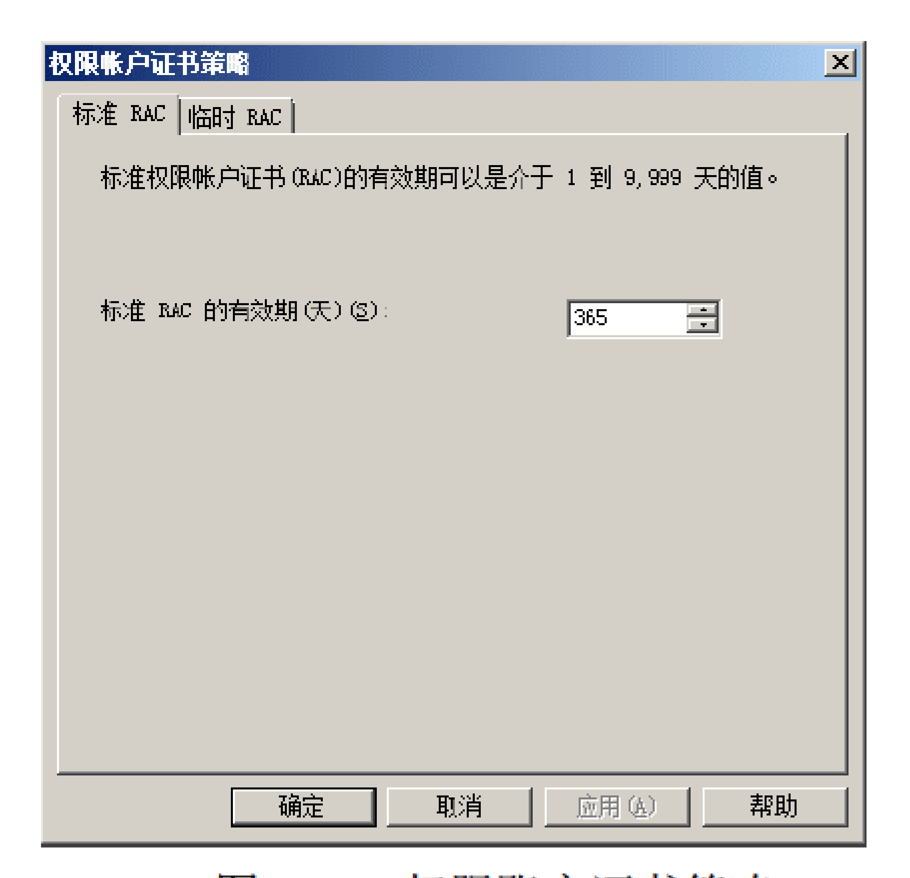


图 9-84　权限账户证书策略

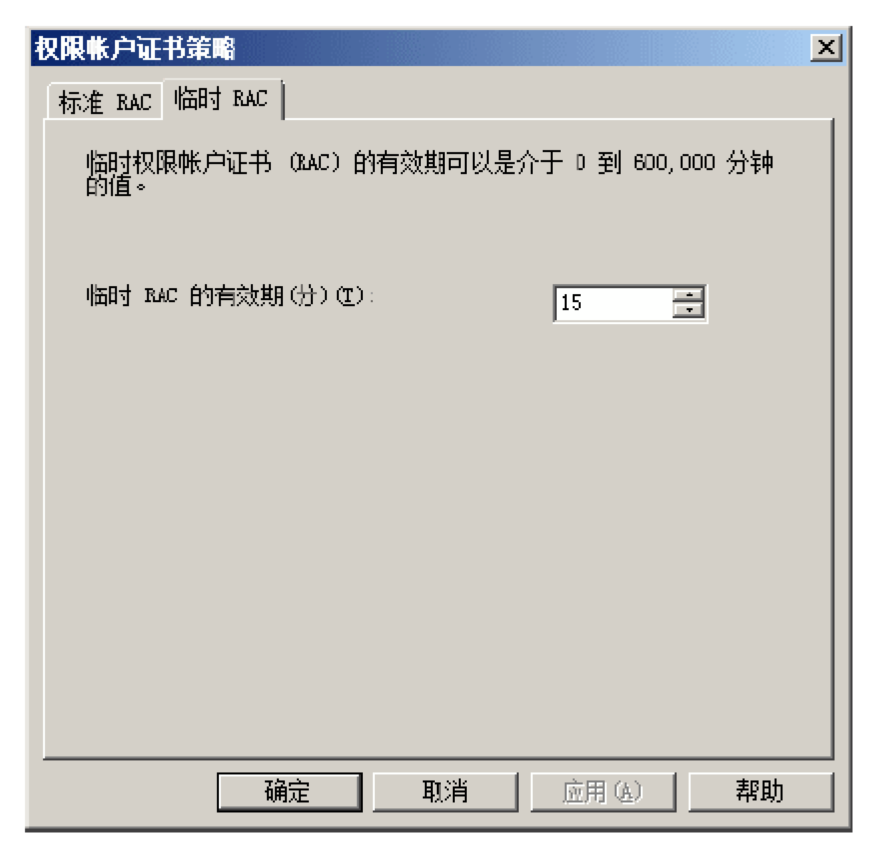


图 9-85　临时 RAC

9.5.4　配置排除策略

排除策略的功能是防止非授权用户使用 AD RMS 服务，可供用户使用的排除策略包括用户、应用程序、密码箱版本和 Windows 版本。默认情况下这些策略都是不启用的，配置之前应先将其启用。排除策略排除某个实体后，AD RMS 服务器创建的用户许可证将在排除列表中列出该实体。如果一段时间后决定删除某个以前包含在排除策略中的实体，只须在“排除策略”窗口的相应列表中将其删除即可。任何获取新证书的请求或授权请求都不会将该实体当作已排除实体。

在 AD RMS 控制台窗口中，选择“排除策略”选项，显示如图 9-86 所示“排除策略”窗口，可以设置用户、应用程序、密码箱及 Windows 版本排除。



说 明

建议不要从排除策略中删除实体，除非可以确定在创建排除策略前颁发的所有证书都已到期。否则，新旧证书都允许对内容解密，将留下非常严重的安全隐患。

图 9-86 “排除策略”窗口

1. 用户排除

用户账户排除可用于排除已经存在安全隐患的信任用户，如某用户账户原本是可信的，但其 AD RMS 凭证不慎泄露，其他非授权用户则可能通过此凭证使用受 AD RMS 保护的文档。此时就可以通过排除该用户的权限账户证书的公钥来排除该证书。排除权限账户证书后，下次该用户试图获得新内容的用户许可证时，其请求将被拒绝。要获得用户许可证，该用户必须使用新的密钥对来检索新的权限账户证书。

要排除根认证服务器或群集上的权限账户证书，可以在根认证服务器的“排除策略”中指定用户的域账户，并且应当在通过注册子过程注册的所有服务器上同时排除其权限账户证书。用户排除策略的具体步骤如下所示。

01 在 AD RMS 控制台窗口的左侧栏中，展开“排除策略”，选择“用户”选项，显示如图 9-87 所示窗口。默认状态下，用户排除为禁用状态。

02 在右侧的“操作”栏中单击“启用用户排除”链接，即可启用用户排除策略，如图 9-88 所示。

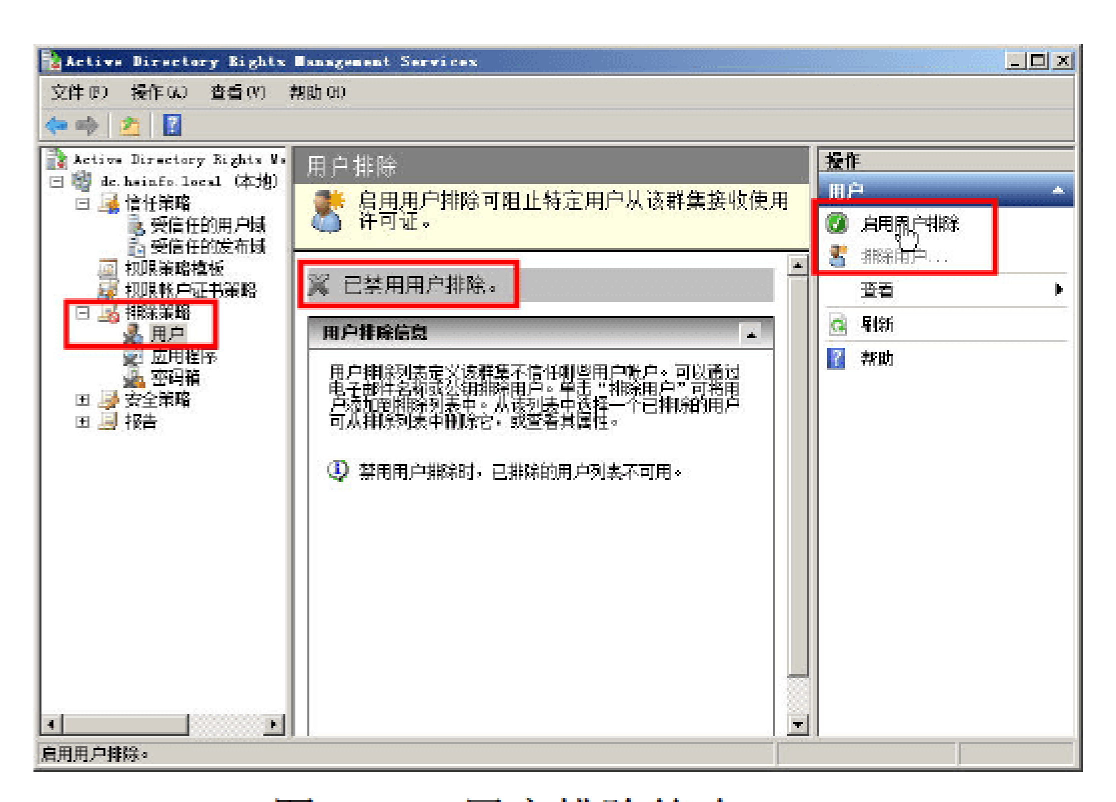


图 9-87 用户排除策略

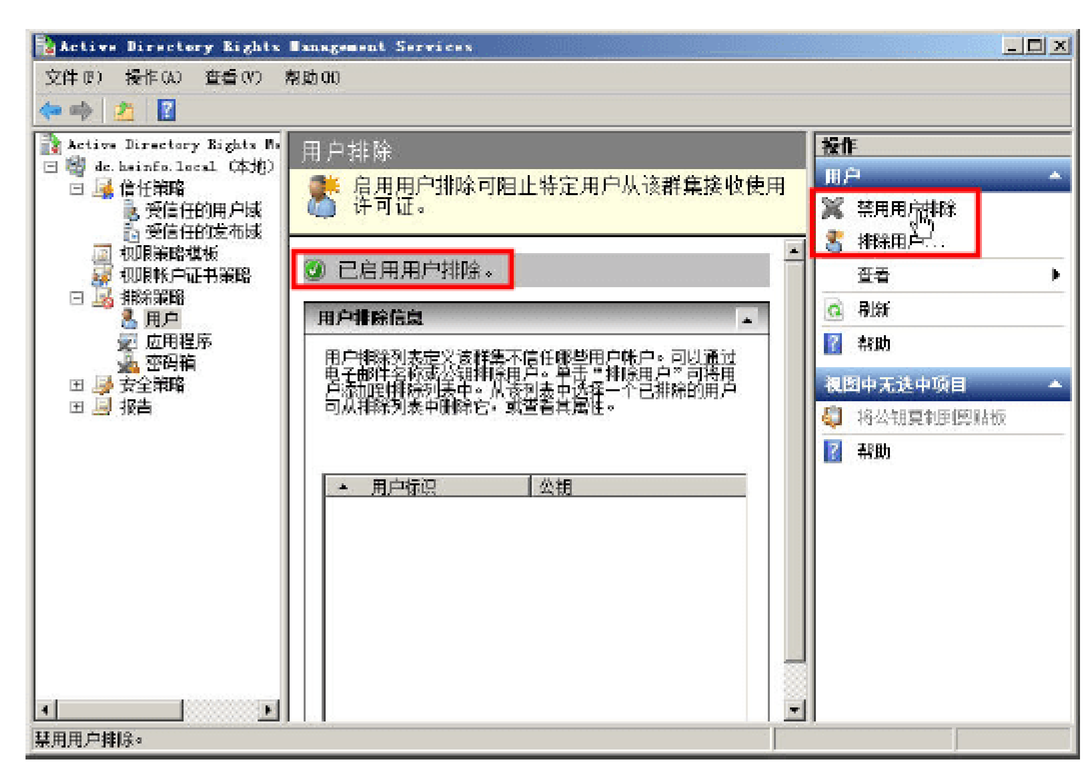


图 9-88 启用用户排除策略

03 单击“操作”栏中的“排除用户”链接，显示如图 9-89 所示“添加要排除的用户”对话框，可以通过用户名或者用户账户证书的公钥字符串进行排除。

04 单击“完成”按钮，用户排除成功。



图 9-89　“添加要排除的用户”对话框

2. 应用程序排除

排除应用程序的主要依据是应用程序的类型及版本号范围。一旦配置应用程序排除策略后，将在每个用户许可证中添加一个条件限制，即如果请求该许可证的应用程序不在已排除列表中，那么该许可证只能绑定到它所针对的受 AD RMS 保护的内容。应用程序排除在很多情况下都是非常实用的，通常情况下，应用程序版本越低，其安全性也越差。通过应用程序排除，就可以限制 AD RMS 服务器为运行较低版本应用程序的客户端提供许可证，以保证文档内容的安全。应用程序排除的具体步骤如下所示。

01 在 AD RMS 控制台窗口的左侧栏中，展开“排除策略”，选择“应用程序”选项，单击“启用应用程序排除”链接，即可启用应用程序排除策略，如图 9-90 所示。

02 在右侧的“操作”栏中单击“排除应用程序”链接，显示如图 9-91 所示“添加要排除的应用程序”对话框。在“应用程序文件名”文本框中，输入应用程序的名称，例如 Office Word 2003；利用“最低版本”和“最高版本”来限定版本范围，必须采用四位数字的句点分隔格式，不足四位则用零补齐，例如 1.2.3.0。本例中，最低版本为 11.5604.5606.0，是未安装 SP2 和 SP3 的 Office，而 11.8169.8172.0 则是 Office 最高版本。

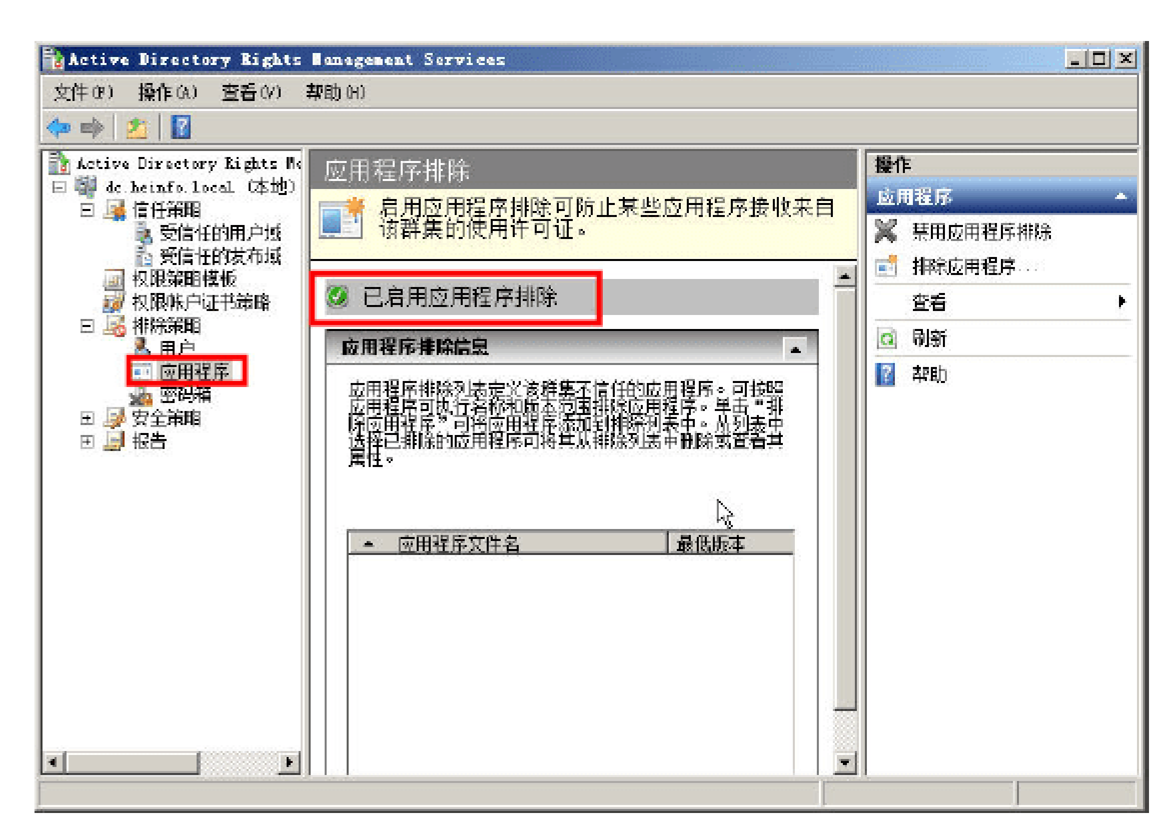


图 9-90　应用程序排除

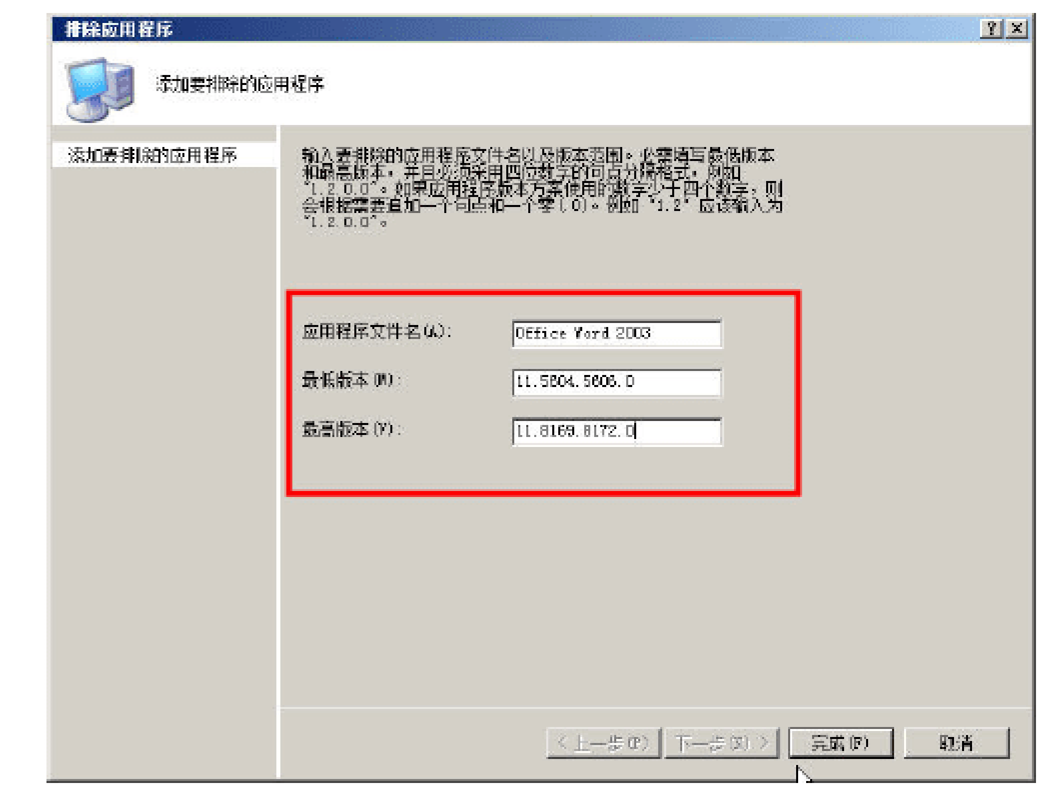


图 9-91　添加要排除的应用程序

03 单击“完成”按钮，应用程序排除完成。

3. 密码箱版本排除

密码箱的功能是为客户端提供加密和解密，以保证私钥的安全。密码箱版本低于 AD RMS 指定版本的客户端，将无法从该群集获得权限账户证书或使用许可证。当启用根据密码箱版本进行排除的功能以后，使用低于指定版本的密码箱软件的客户端将无法获得权限账户证书或用户许可证，原因是其请求将被拒绝。这些客户端必须安装新版本的 AD RMS 客户端软件，以获得使用当前版本软件的新密码箱。

01 在 AD RMS 控制台窗口的左侧栏中，在“排除策略”窗格中选择“密码箱”选项，单击右侧“操作”栏中的“启用密码箱排除”链接，即可启用该排除策略，如图 9-92 所示。默认最小密码箱版本为“未设置”。



说 明

单击“查看推荐的最小密码箱版本”链接，将自动登录微软网站，并显示最小密码箱版本信息，如图 9-93 所示。

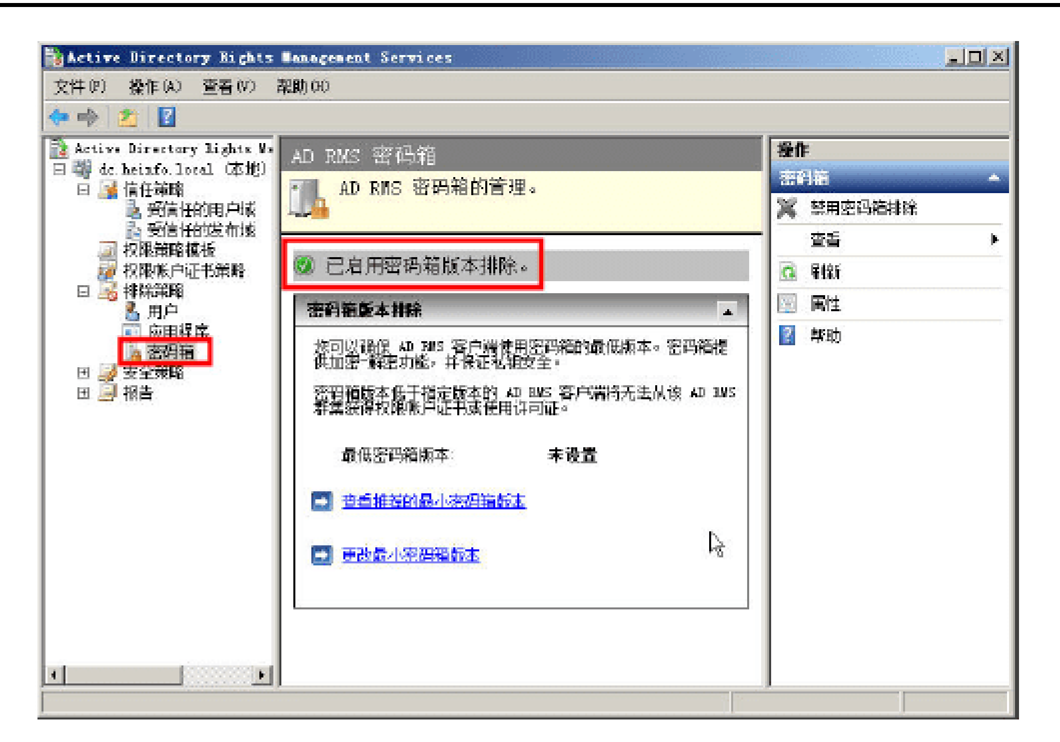



图 9-92 密码箱版本排除

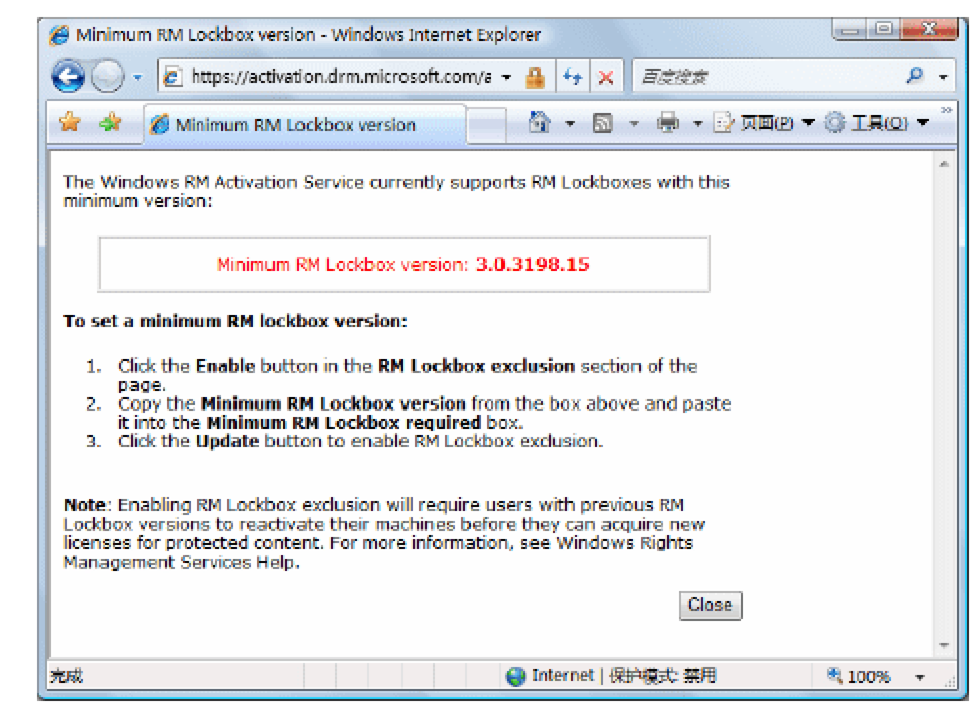


图 9-93 查看密码箱版本

02 单击“更改最小密码箱版本”链接，显示如图 9-94 所示“密码箱”对话框。在“最小密码箱版本”文本框中输入微软网站反馈的版本信息即可。为了确保服务器的安全，建议在普通客户机登录该站点来查找反馈信息。

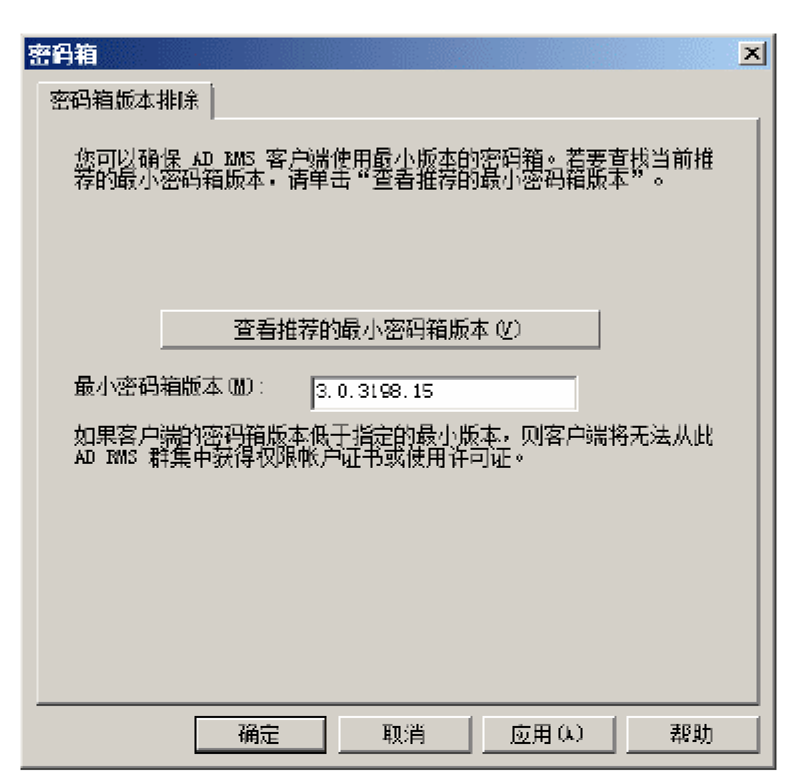


图 9-94 密码箱

03 单击“确定”按钮，密码箱版本排除成功。

4. Windows 版本排除

对于 Windows 98/Me 操作系统来说，支持早期 RMS 1.0 客户端，但不支持 NTLM 身份验证。因此，为了防止用户在运行上述操作系统的计算机上使用受 AD RMS 保护的文档，可以启用 Windows 版本排除策略，使用户只能使用高于 Windows Me 的 Windows 版本。

在 AD RMS 控制台窗口的左侧栏中，在“排除策略”窗格中单击“Windows 版本”，显示“Windows 版本”窗口。单击右侧“操作”栏中的“启用 Windows 版本排除”链接，即可启用 Windows 版本排除策略，如图 9-95 所示。

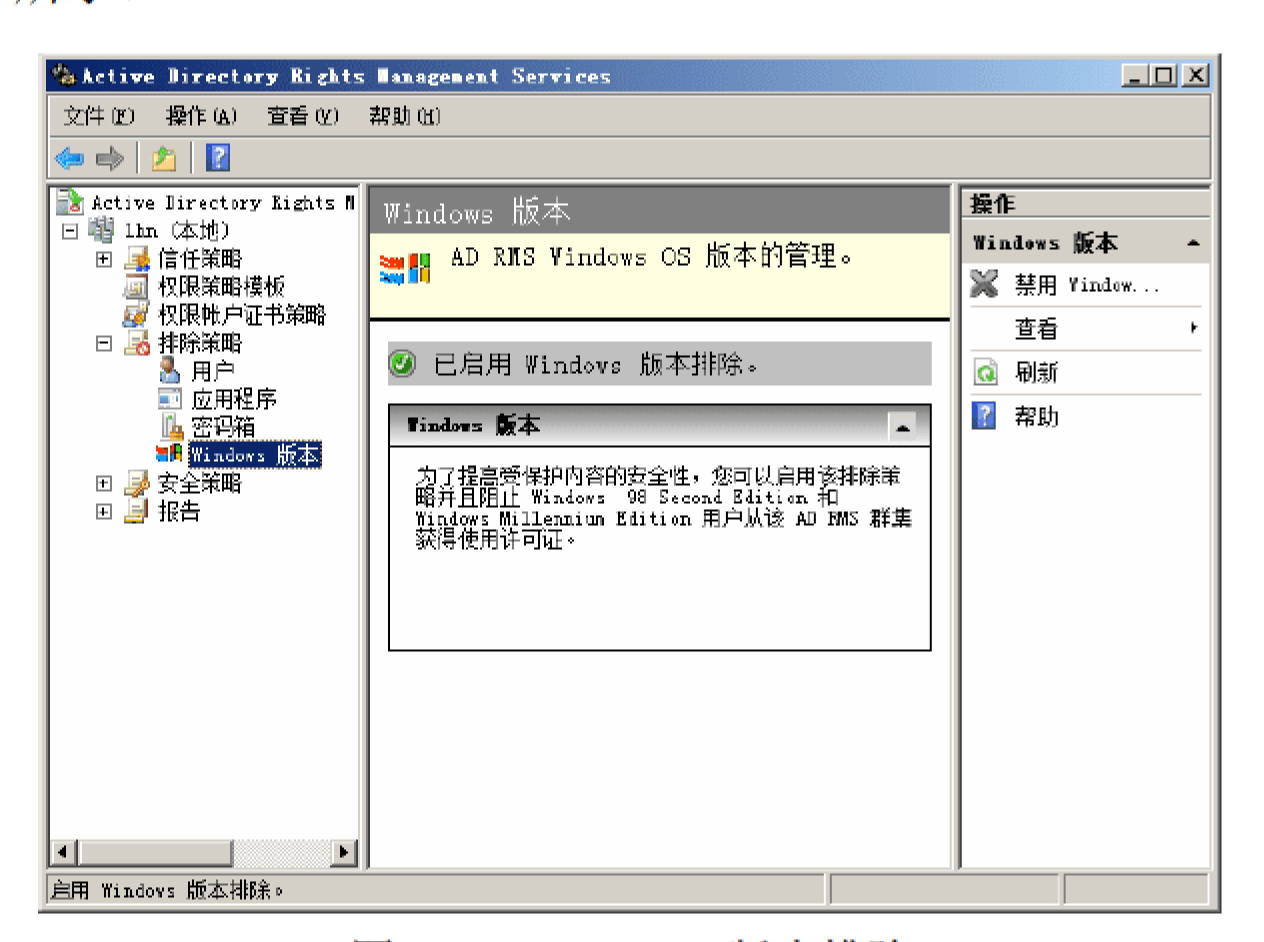


图 9-95　Windows 版本排除

当设置了基于 Windows 版本来排除用户的排除策略以后，所有用户许可证中都将包含相应条件，这些条件可防止运行 Windows 98/Me 的客户端使用这些许可证。

9.5.5　配置安全策略

在“AD RMS 控制台”窗口的左侧栏中，选择“安全策略”，显示如图 9-96 所示“安全策略”窗口，包括超级用户、群集密钥密码和解除授权 3 种策略。同样，默认状态下，所有策略都是禁用的，配置之前必须先将其启用。

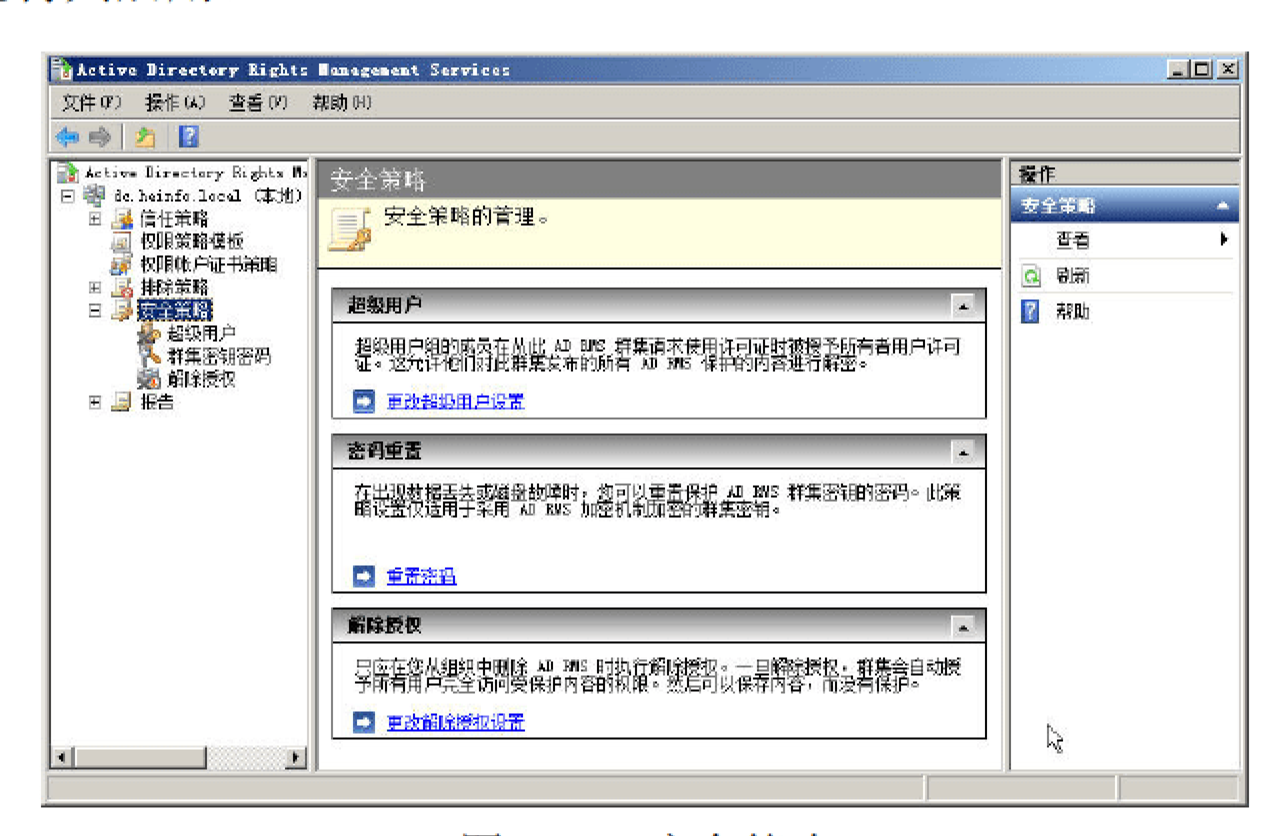


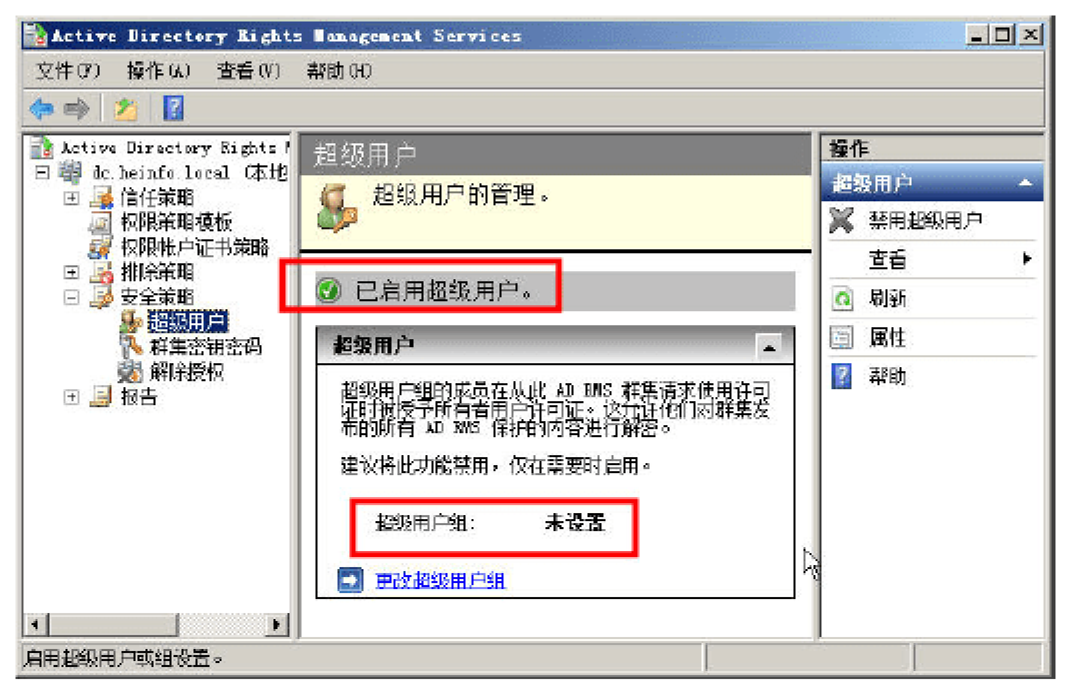
图 9-96　安全策略

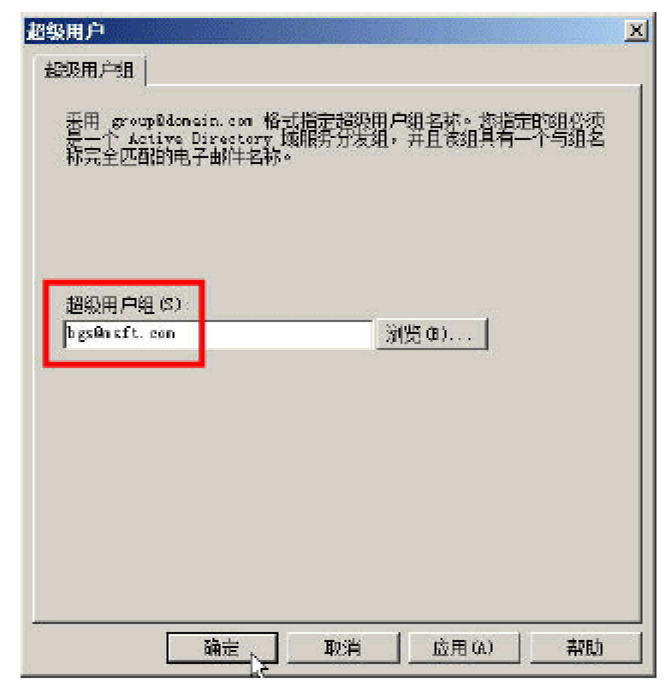
1．超级用户策略

超级用户组的成员在从 AD RMS 请求用户许可证时，被授予了所有者用户许可证，允许他们使用该服务器的所有受 RMS 保护的内容。超级用户策略配置步骤如下。

01 在“AD RMS 控制台”窗口的左侧栏中，选择“超级用户”选项，在“操作”栏中单击“启用超级用户”链接，启用超级用户，如图 9-97 所示。默认情况下，超级用户组为“未设置”。

02 单击“更改超级用户组”链接，打开如图 9-98 所示“超级用户”对话框。在“超级用户组”文本框中输入该 Active Directory 林中现有组的完全限定的域名即可。

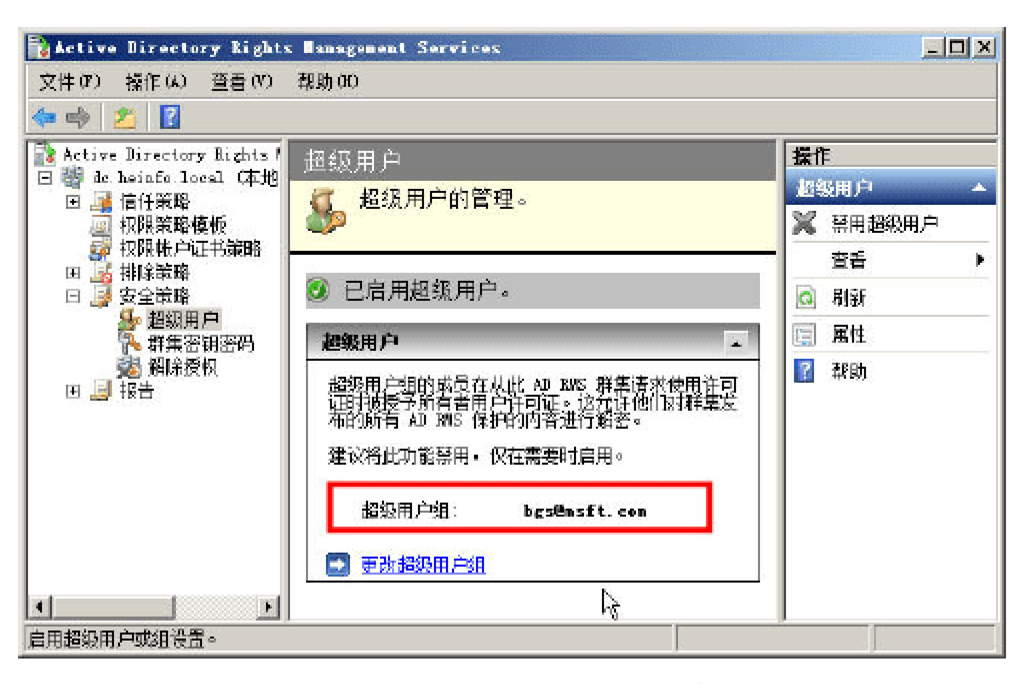

图 9-97　启用超级用户


图 9-98　“超级用户”对话框


说 明

必须事先在域控制器上，为用户组配置好电子邮件名称，否则将无法正常添加。

03 单击“确定”按钮，即可更改超级用户组，如图 9-99 所示。


图 9-99　更改超级用户组

2. 群集密钥密码

通过设置群集密钥密码，AD RMS 将为服务器创建 AD RMS 私钥，该私钥将被加密并存储在配置数据库中。建议将私钥备份并存储在一个安全的位置。此外，还可考虑使用硬件安全模块来加强 AD RMS 私钥的安全性，因为此密钥将用于受 AD RMS 服务器保护的所有内容的加密模式。如果 AD RMS 私钥由于某种原因被泄漏，则需要在服务器上取消设置 AD RMS，然后再次设置 AD RMS 以获得新的私钥。群集密钥密码策略配置步骤如下。

01 在“AD RMS 控制台”窗口的左侧栏中，选择“群集密钥密码”选项，如图 9-100 所示。在此处可以看到密钥保护方法为“AD RMS 集中管理”。



图 9-100　群集密钥密码设置

02 单击“更改群集密钥密码”链接，显示如图 9-101 所示“群集密钥密码”对话框。分别在“密码”和“确认密码”文本框中输入新的密钥密码即可。

03 单击“确定”按钮，显示如图 9-102 所示提示框，提示密码已成功重置。单击“确定”按钮即可。

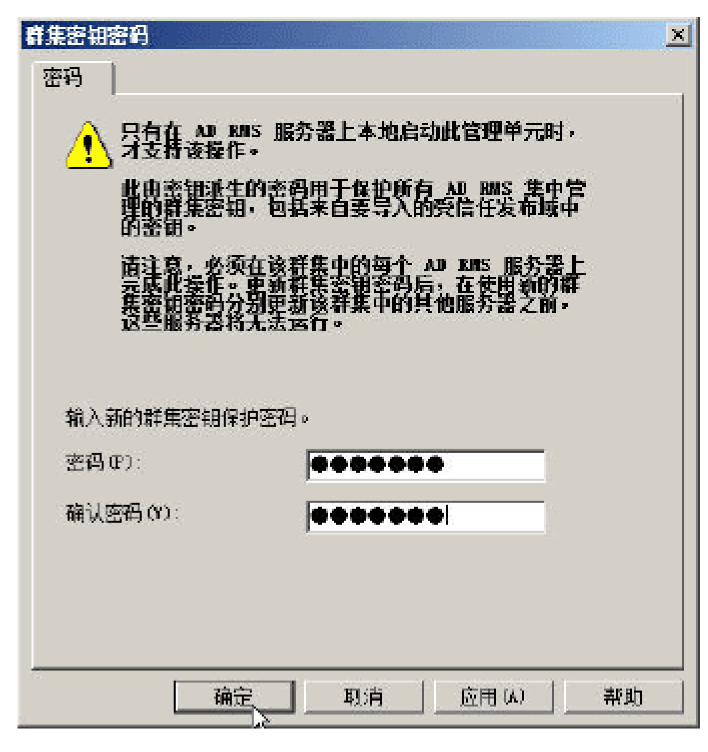
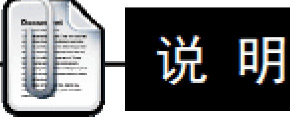


图 9-101　群集密钥密码



图 9-102　密码已成功重置



说 明

如果该服务器曾用来保护内容，则应通知所有内容所有者，同时使用设置了新私钥的 AD RMS 服务器来重新发布内容。使用受已泄漏的私钥保护的所有内容副本都应销毁，因为这些内容无法受到足够的保护。

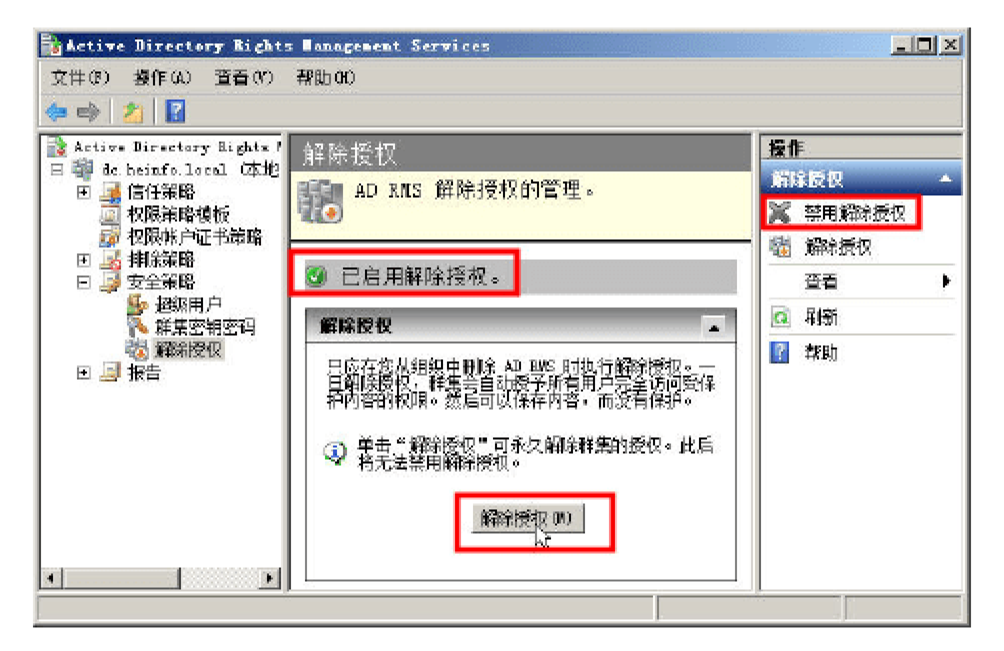
3. 解除授权

解除授权是指撤销 AD RMS 服务器赋予指定用户对被保护文档的所有权限，即所有用户都具有完全访问的权限。因此，通常都是删除 AD RMS 服务器群集时才执行解除授权操作。解除授权的主要操作步骤如下。

01 在“AD RMS 控制台”窗口的左侧栏中，在“安全策略”中选择“解除授权”选项，显示“解除授权”窗口。默认状态下，“解除授权”为禁用状态，并且“解除授权”按钮为灰色不可

用状态。单击“操作”栏中的“启用解除授权”链接，启用解除授权策略，同时，“解除授权”按钮变为可用状态，如图 9-103 所示。

02　单击“解除授权”按钮，显示如图 9-104 所示“确认解除授权”提示框。提示如果解除 AD RMS 群集的授权，需要重新安装和配置 AD RMS 群集。



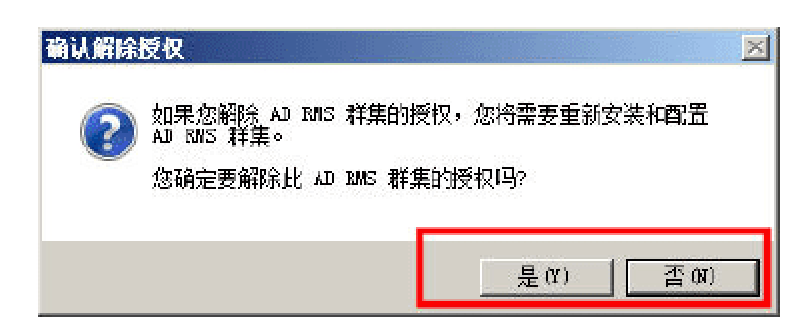


图 9-103　启用解除授权　　　　图 9-104　确认解除授权

03　单击“是”按钮即可解除授权，如图 9-105 所示。本地 AD RMS 群集的所有配置选项都已经被删除了。

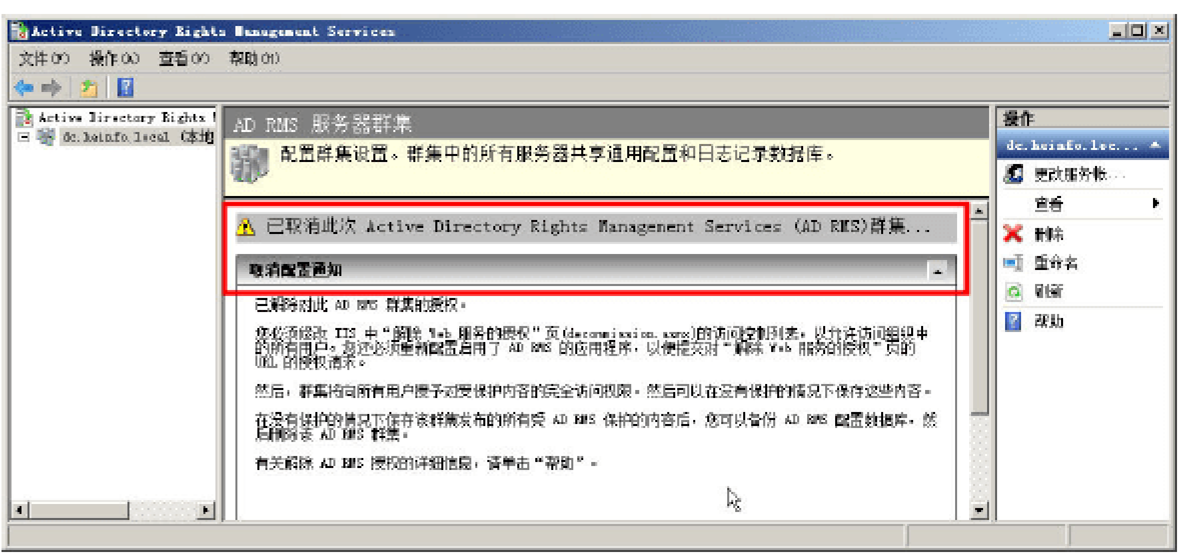


图 9-105　成功解除授权

解除授权后，AD RMS 服务器的操作将会发生改变，它能够提供一个密钥，用于解密以前发布的受保护的内容。通过此密钥，可在不使用 AD RMS 保护方法的情况下保存内容。

04　解除授权之后，还必须修改 IIS 中“解除 Web 服务的授权”页（decommission.asmx）的访问控制列表，以允许所有用户访问。在“IIS 管理器”窗口中找到 decommission.asmx 页，并打开如图 9-106 所示“身份验证”对话框，取消原有的各种身份验证方式，并启用“匿名身份验证”。

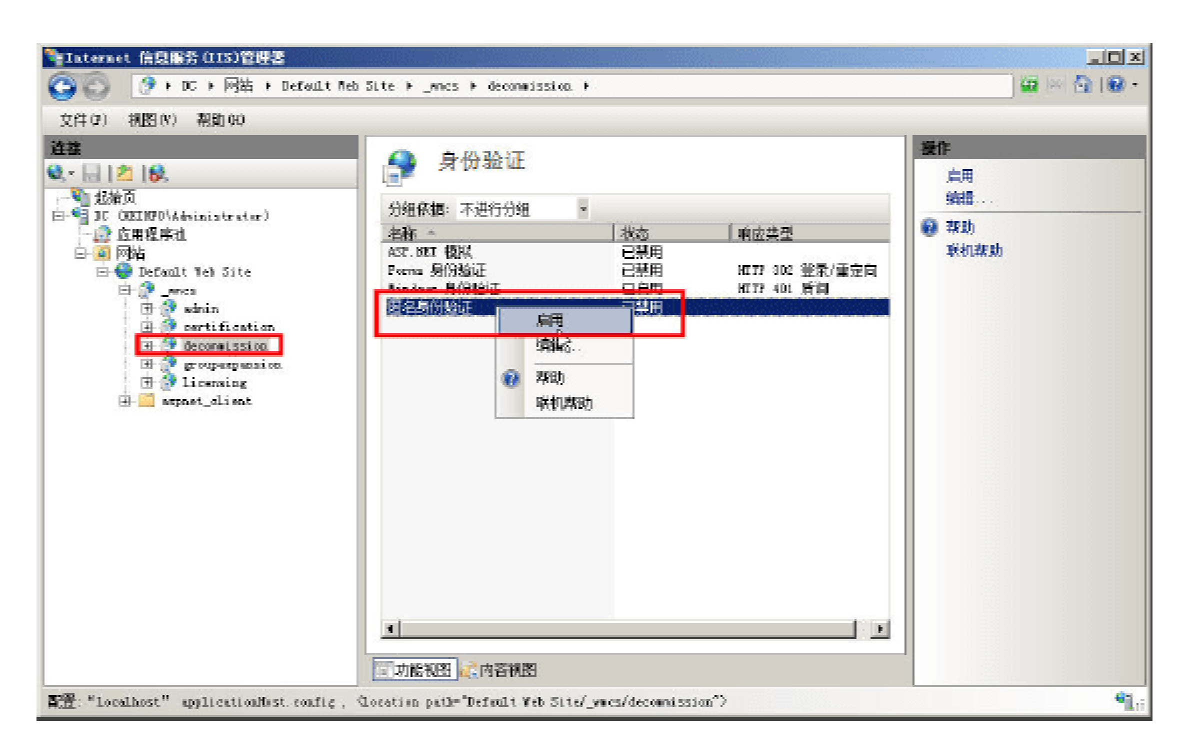


图 9-106　取消 IIS 中的身份验证机制

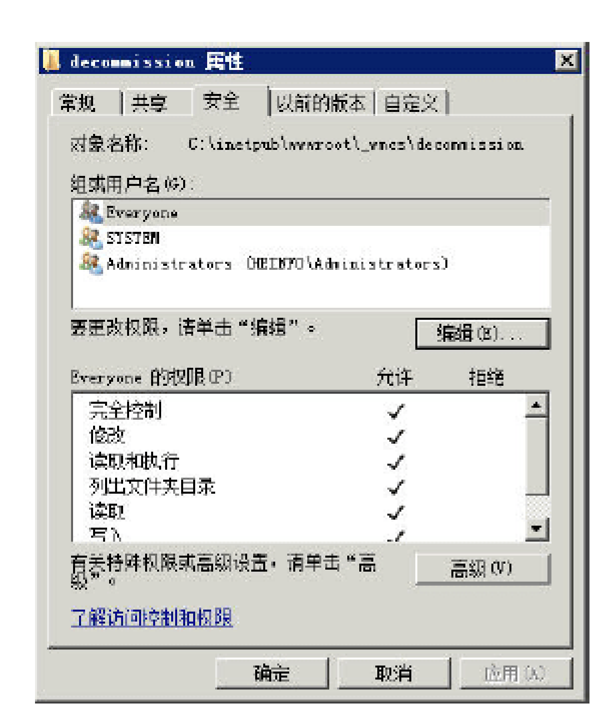


图 9-107　修改 Everyone 的权限

05 还要打开 decommission.asmx 页所在的目录（通常在 C:\inetpub\wwwroot_wmcs\ decommission），添加 Everyone 用户组对该目录具有“完全控制”权限，如图 9-107 所示。

9.6　卸载 AD RMS 服务器端

如果在安装 AD RMS 服务器的时候，出现了类似图 9-108 所示的错误，或者有其他的错误，而不能配置 AD RMS 服务器时，可按照下面的步骤将其卸载，然后重新安装。

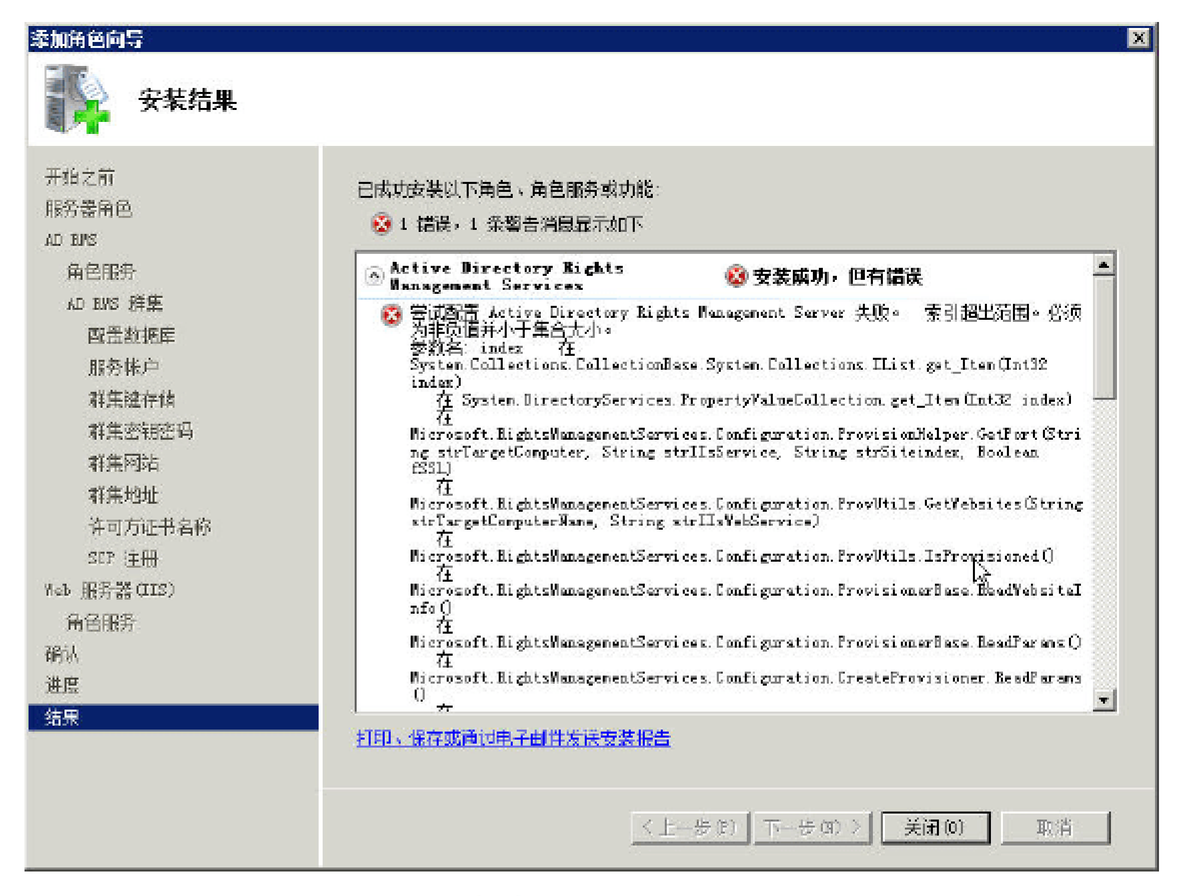


图 9-108　安装 AD RMS 出现错误

卸载 AD RMS 服务器的步骤如下。

01 打开“服务器管理器”，定位到“角色”，在右侧单击“删除角色”按钮，在打开的“删除服务器角色”对话框中，取消选中“Active Directory Rights Management Services”复选框，如图 9-109 所示。

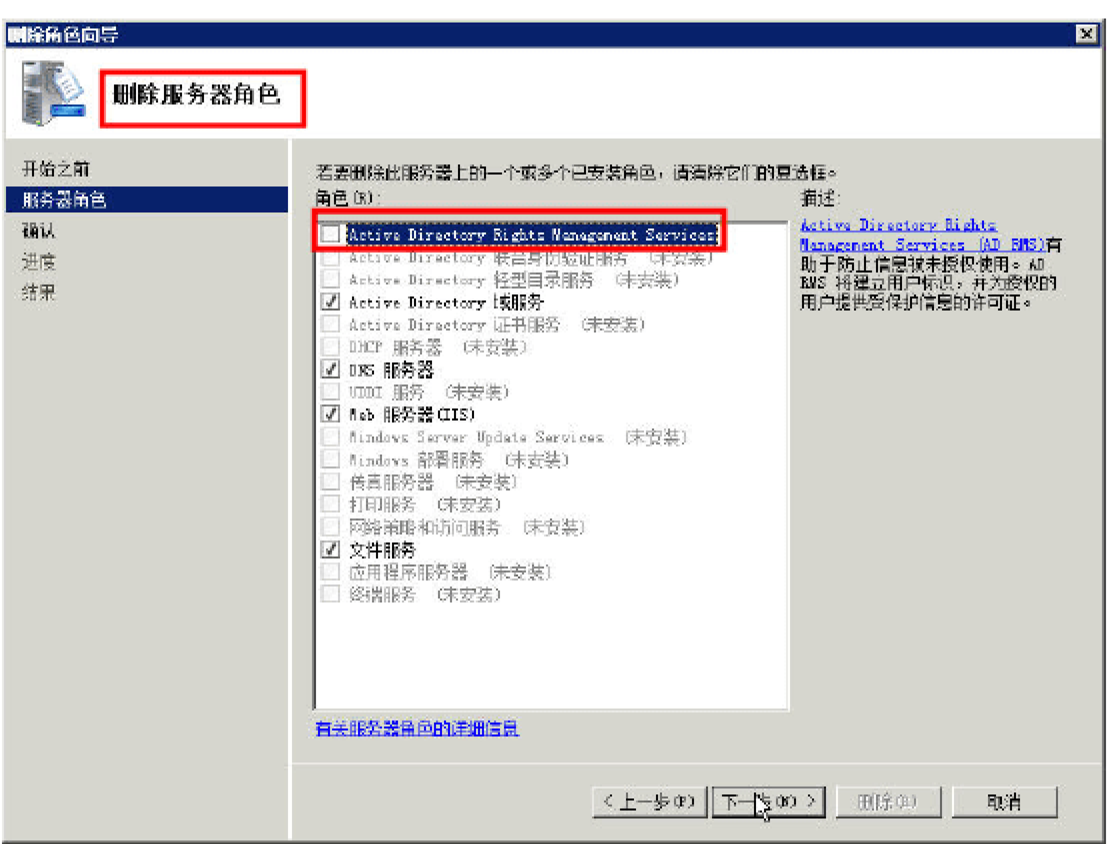
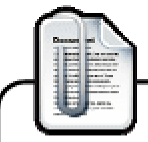


图 9-109　取消 AD RMS



说 明

不能同时取消选中“Web 服务器（IIS）”复选框，否则在卸载之后，会出现如图 9-110 所示的错误，导致 AD RMS 服务器不能卸载。

02 卸载 AD RMS 服务器之后，根据提示重新启动计算机，如图 9-111 所示。



图 9-110　删除失败

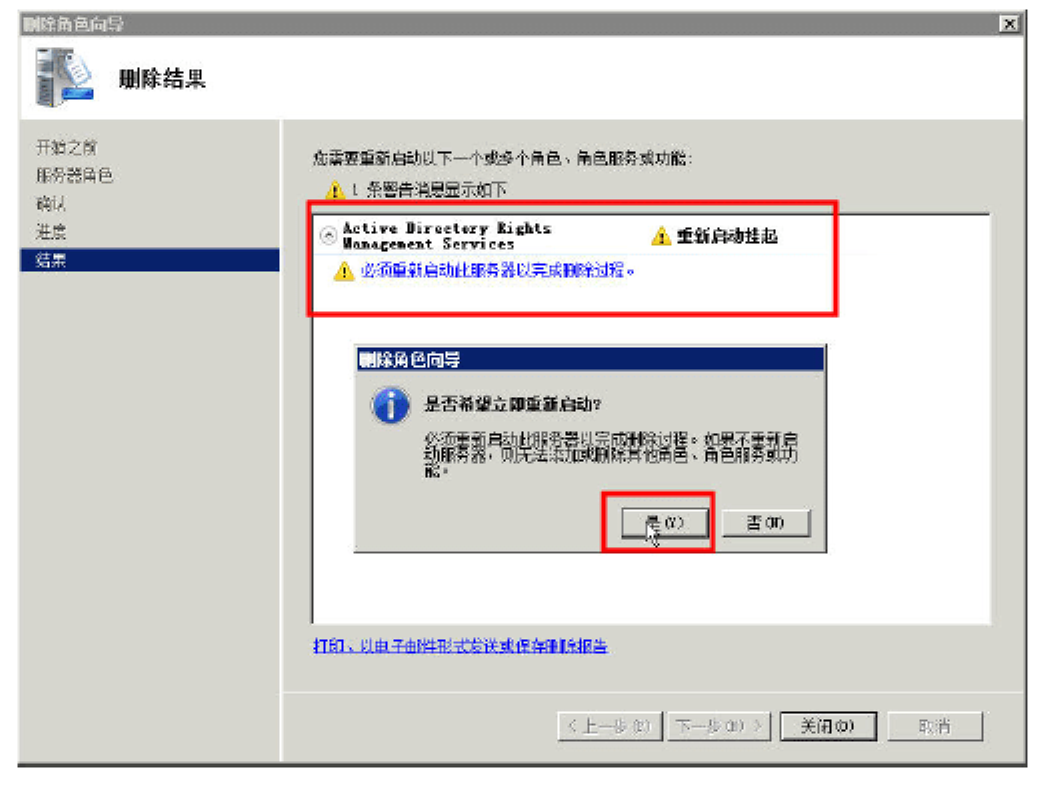


图 9-111　卸载 AD RMS 之后重新启动

03 再次进入系统之后，在“服务器管理器”中选择“删除角色”选项，在“删除服务器角色”对话框中，卸载“Web 服务器（IIS）”，如图 9-112 所示。

04 卸载 Web 服务器之后，根据提示重新启动计算机，如图 9-113 所示。



图 9-112　卸载 IIS

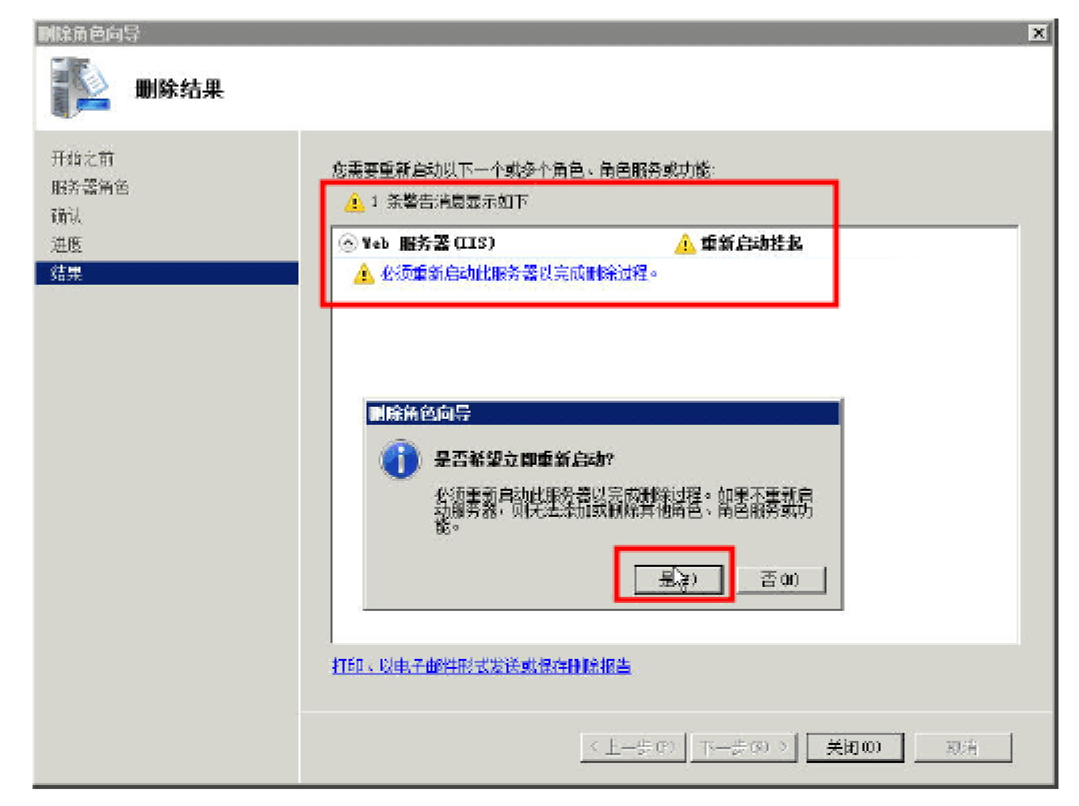


图 9-113　重新启动完成 Web 服务器的卸载

05 再次进入系统后，在“服务器管理器”中，选择“删除功能”选项，在“删除功能向导”对话框中，取消选中“Windows 进程激活服务”和“Windows 内部数据库”复选框，如图 9-114 所示。

06 卸载之后，根据提示，重新启动计算机，如图 9-115 所示。

07 再次进入系统后，打开“资源管理器”，删除 intepub 目录，如图 9-116 所示。

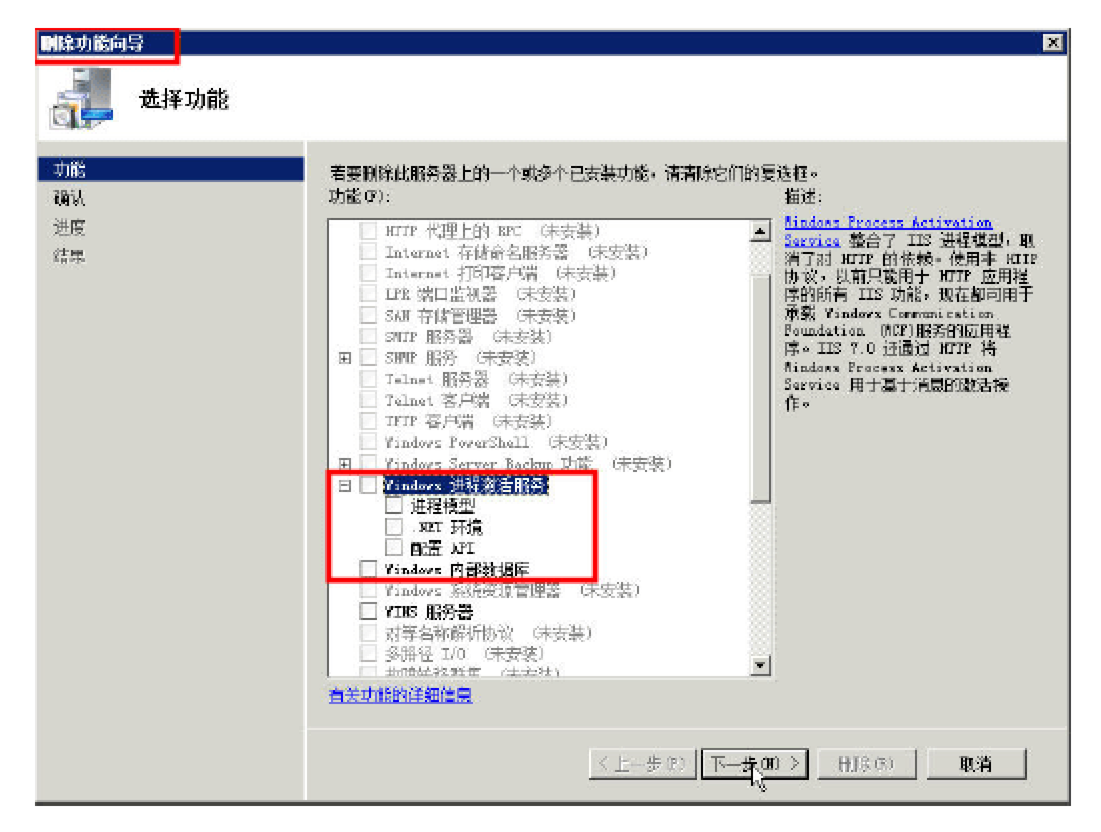


图 9-114　删除 Windows 内部数据库

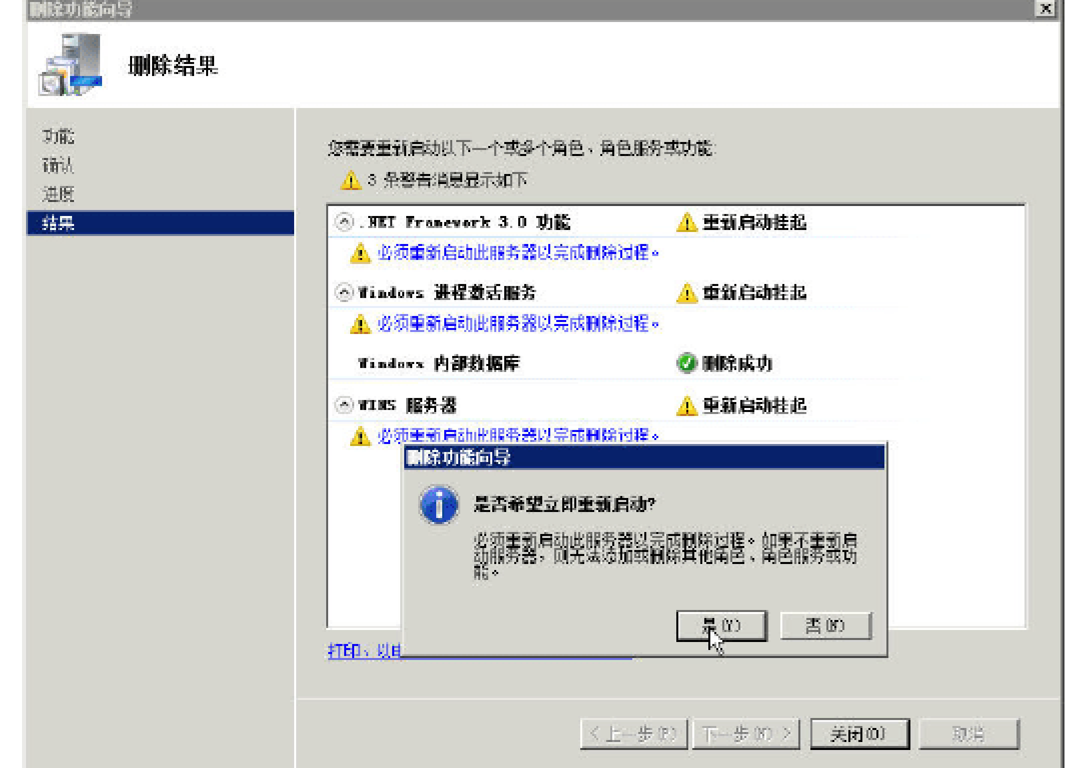


图 9-115　重新启动以完成卸载

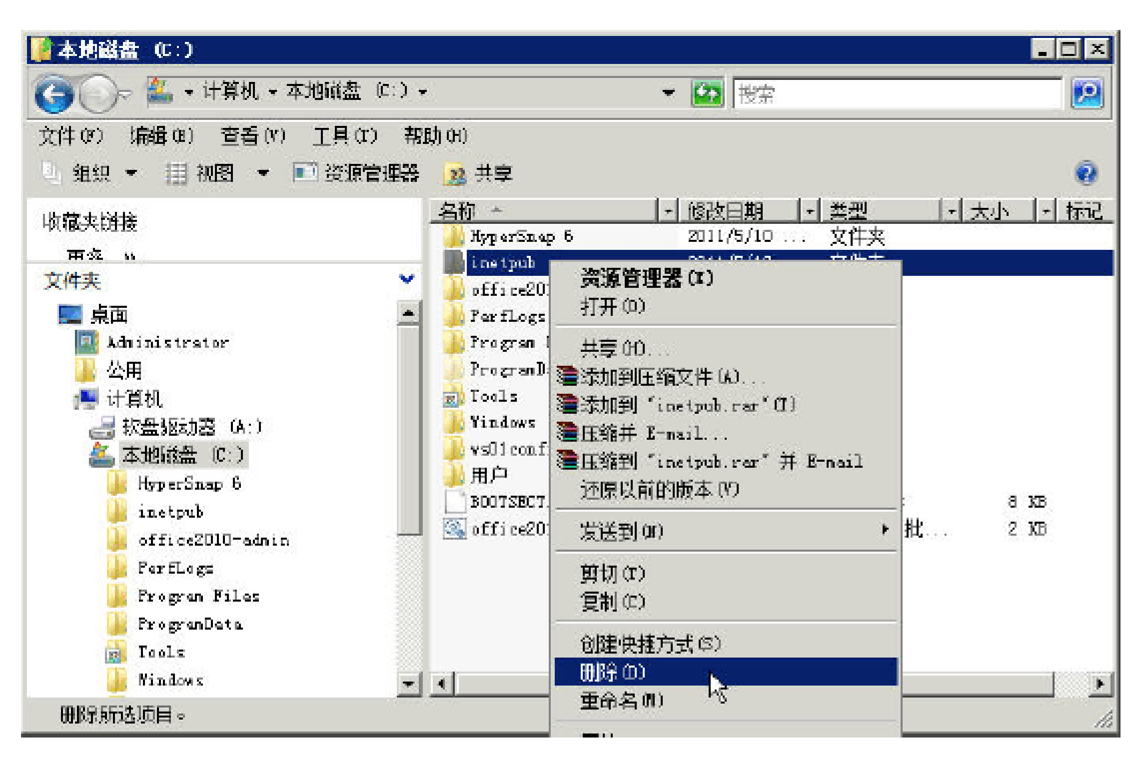


图 9-116　删除 Web 服务器默认目录

完成上述操作后，重新安装 AD RMS 服务器即可。

第 10 章 DFS 分布式文件系统管理与应用

使用分布式文件系统（Distributed File System，简称 DFS），可以让用户很方便地访问和管理物理上分布在网络各处的文件。通过 DFS，可以使分布在多个服务器上的文件如同位于网络上的同一个位置那样显示在用户面前。用户在访问文件时不再需要知道和指定它们的实际物理位置。分布式文件系统（DFS）命名空间和 DFS 复制对文件、负载共享和 WAN 提供了友好而可用性高的访问。

例如，如果有 3 台服务器，每个服务器都有多个共享文件夹。对于用户来说，使用每个服务器上的每个共享文件夹，都要创建一个“网络驱动器”进行映射。而使用“分布式文件系统”，只需要访问一个共享（分布式文件系统的根目录），并创建一个驱动器映射，就可以访问分布在多个服务器上的多个不同的共享文件夹了。

10.1 Windows Server 2008 R2 中的 DFS 改进

分布式文件系统是从 Windows 2000 Server 开始提供的服务，它还可以自动在多台服务器之间同步数据，但截止到 Windows Server 2003 R2 之前的系统（包括 Windows Server 2003），DFS 中的“同步数据”并不是很好用，并且 DFS 复制对带宽的依赖也比较高。基于此，Windows Server 2003 R2 重写了 DFS 的部分程序，并对原来的 DFS 做了比较大的改进，提高了 DFS 的可用性。在 Windows Server 2003 R2 操作系统中，Microsoft 修改并重命名了 DFS 命名空间（以前称为 DFS），用 DFS 管理单元替换了分布式文件系统管理单元，并引入了新的 DFS 复制功能。在 Windows Server 2008 操作系统中，Microsoft 添加了 Windows Server 2008 模式的基于域的命名空间，并且大幅改进了可用性和性能。在 Windows Server 2008 R2 操作系统中，Microsoft 增加了大量功能，并对现有功能进行了改进。

本章将以 Windows Server 2008 的 DFS 为例，介绍 DFS 文件系统在企业网络中的应用。



说 明

在本章的内容中，需要使用 3 台 Windows Server 2008 R2 的虚拟机来做实验，用户可以从 Hyper-V 中导出的 Windows Server 2008 R2 虚拟机、然后按不同名称导入两次，以添加两个虚拟机。再使用导入的虚拟机并启动后，运行 sysprep 重新生成 SID 并修改计算机的名称即可。有关虚拟机的“导出”与“导入”，请参见本书第 11 章的相关内容。在本章中，实验拓扑如图 10-1 所示。

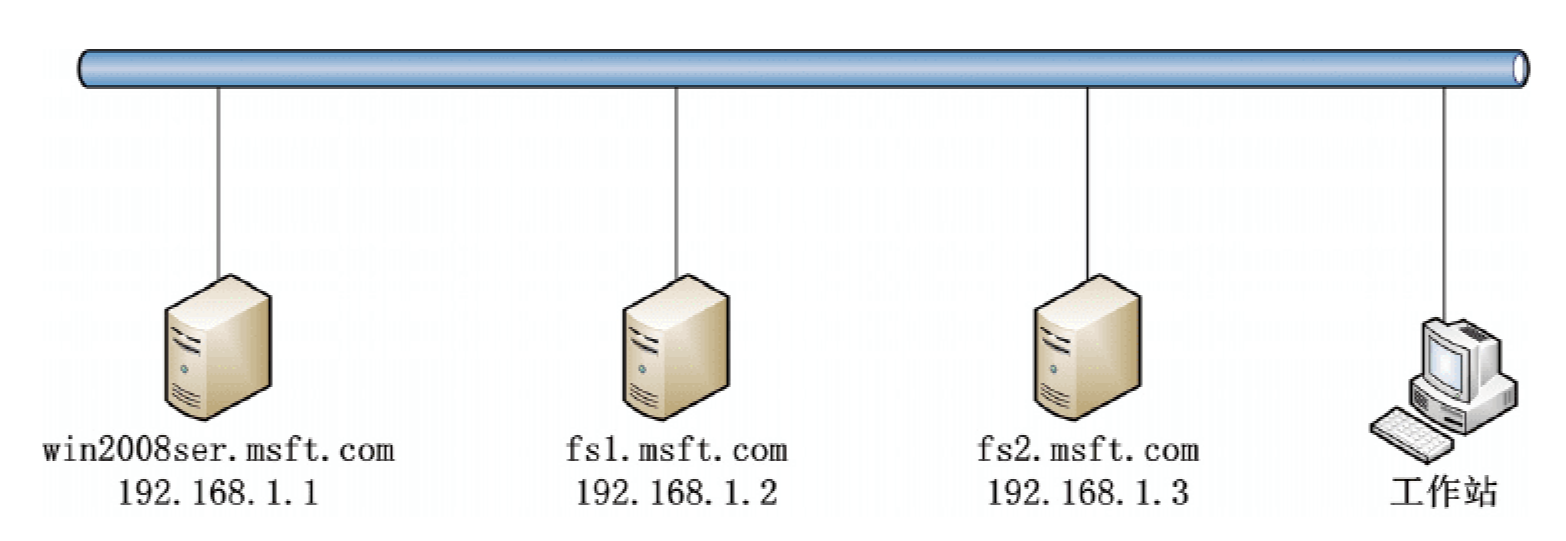


图 10-1　DFS 实验拓扑图

在 Windows Server 2008 中，DFS 服务有了重大改进，如下所示。

- 支持数据汇聚。
- 访问基于枚举，只允许用户看到文件服务器中赋予了相应存取权限的文件和文件夹。默认情况下，这一功能在命名空间中并未启用（尽管创建新的共享文件夹时这项功能被默认启用），并且只支持运行着 windows server 2008 系统的主机上的单机 DFS 命名空间，或者是基于活动目录的模式。
- 集群支持，支持在 DFS 管理单元中建立独立的命名空间，容错功能更加强大。
- 改进命令行工具，Windows Server 2008 中的 DFS 命名空间包括一个更新版本的 dfsUtil 指挥和新 dfsdiag 命令，该命令可以使用名称诊断。
- Windows Server 2008 支持创建基于域模式的命名空间，增加了对基于枚举的访问的支持及可扩展性，而且支持只读域控制器。
- 繁殖报告，DFS 管理包括一个新的类型的诊断报告，称为繁殖报告。此报告显示在繁殖试验中创建复制的进展测试文件。
- 即时复制，DFS 复制的能力包括强制复写立即发生，暂时忽略复制计划。
- DFS 复制可用于 SYSVOL 复制，在 Windows Server 2008 的域功能级别中，DFS 复制作为复制 AD SYSVOL 文件夹的引擎，它完全替代了文件复制服务 FRS。
- DFS 复制的内容新鲜功能，防止服务器离线很长一段时间后书写新的数据时，会再次重新写入过时的数据。
- 改进意外关机处理，在 Windows Server 2008 中，DFS 复制可以更快地恢复意外关机造成的损失。
- 支持数据复制方向调整，默认情况下复制方向为双向，可以设置为单项。

10.1.1　使用 DFS 文件服务器的必要性

很多企业每天都需要处理大量的数据。而在一个局域网内，需要在服务器上保存的数据越来越多，需要考虑的问题也会很多，这包括：

（1）由于数据众多，单台服务器已经不能满足需要。如果把数据保存在多台服务器上，用户在使用、访问数据时，又没有原来单台服务器访问时方便。

（2）对于重要的数据，需要备份。手动备份太麻烦，如果有大量的数据或者需要经常修改的数据，也不能做到定期备份。

（3）很多时候，为了用户数据的安全，在局域网中会为每个用户在服务器上“开辟”一点空

间，让用户把重要的数据保存到服务器上去。但有一些“不自觉”的用户，他们会在服务器上保存电影、音乐、自己的相片等，而到真正保存有用数据时却已经没有空间。

使用 Windows Server 2008 R2 中的“DFS”可以很容易地解决前 2 个问题，而第 3 个问题可由 Windows Server 2008 R2 中的“文件服务器”解决。

10.1.2　组建基于 Windows Server 2008 R2 的“分布式文件系统”

在本章中，配置 DFS 服务器的主要步骤如下。

01 准备 3 台服务器，IP 地址分别是 192.168.1.1、192.168.1.2、192.168.1.3，这 3 台服务器已经升级到 Active Directory，其中第 1 台 Active Directory 服务器域名为 win2008ser.msft.com，第 2 台服务器域名为 fs1.msft.com，第 3 台服务器域名为 fs2.msft.com。其中一台服务器（fs1.msft.com）作为域的“额外域控制器”，另一台服务器（fs2.msft.com）作为域的“成员服务器”。



说 明

这样做的目的是为了让大家验证，作为 DFS 的服务器，可以是域控制器，也可以是加入到域的成员服务器。在实际使用时，DFS 服务器最好是域的“额外域控制器”而不是“成员服务器”。

02 这 3 台服务器安装 Windows Server 2008 R2 Enterprise，第 1 台服务器的计算机名称设置为 win2008ser，第 2、第 3 台服务器的计算机名称分别为 fs1 和 fs2。

03 在第 2 台服务器 fs1 上，运行 dcpromo 命令，成为现在域的“额外域控制器”。在第 3 台服务器 f2 上，加入现有域，作为“成员服务器”。

04 在每台服务器上，添加“分布式文件系统”组件。

05 在每台服务器上创建一些文件夹并设置共享，同时向文件夹中复制一些对应的文档或数据。

由于升级 windows server 2008 服务器到 Active Directory 模式已在前面章节进行介绍，本章不再赘述。下面讲一下安装“分布式文件系统”的具体步骤。

01 打开“服务器管理器”窗口，在左侧的控制台树中选择“角色”选项，然后选对话框右侧的“添加角色”选项，运行“添加角色向导”。

02 在“选择服务器角色”对话框中，选中“文件服务”复选框，如图 10-2 所示。

03 在“选择角色服务”对话框中选中，“分布式文件系统”复选项，如图 10-3 所示。

04 在“创建 DFS 命名空间”对话框中，选择“以后使用服务管理器中的‘DFS 管理’管理单元创建命名空间”单选按钮，

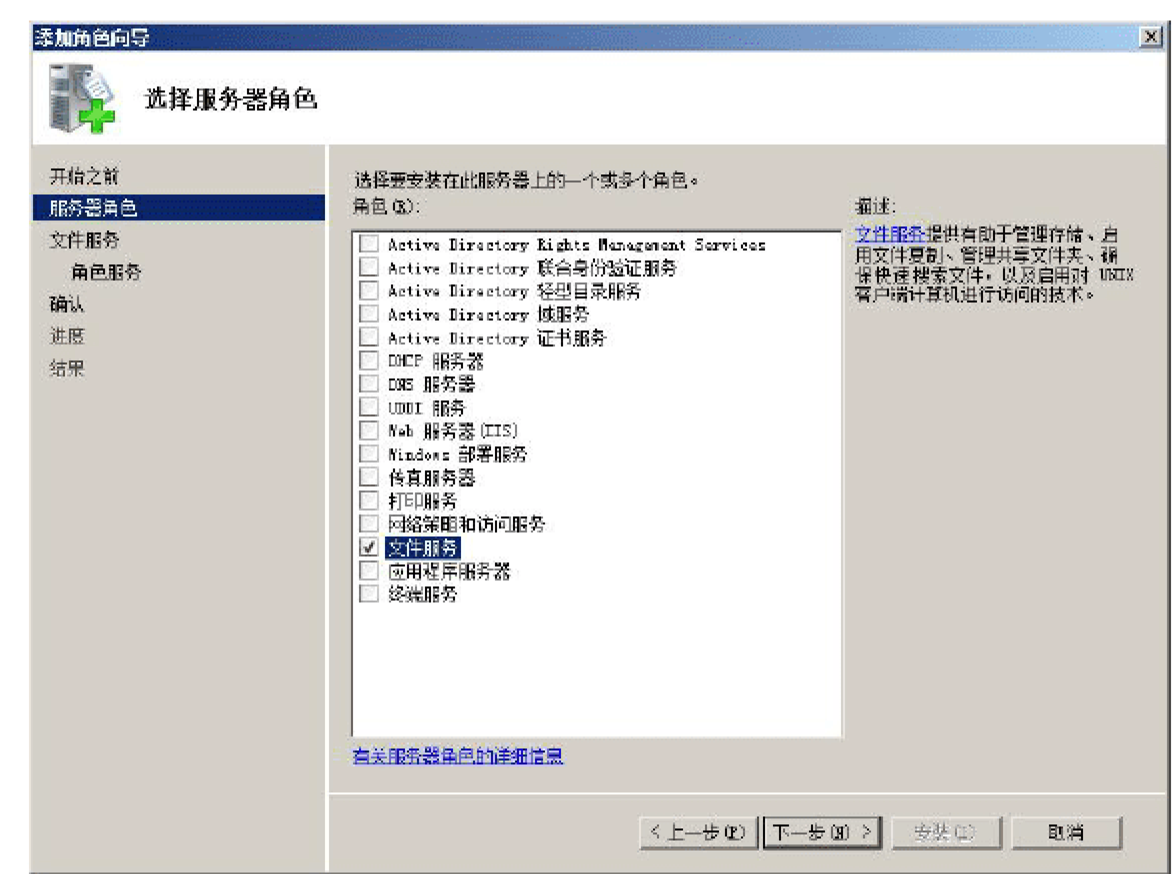


图 10-2　选择文件服务

如图 10-4 所示。



图 10-3　选择角色服务

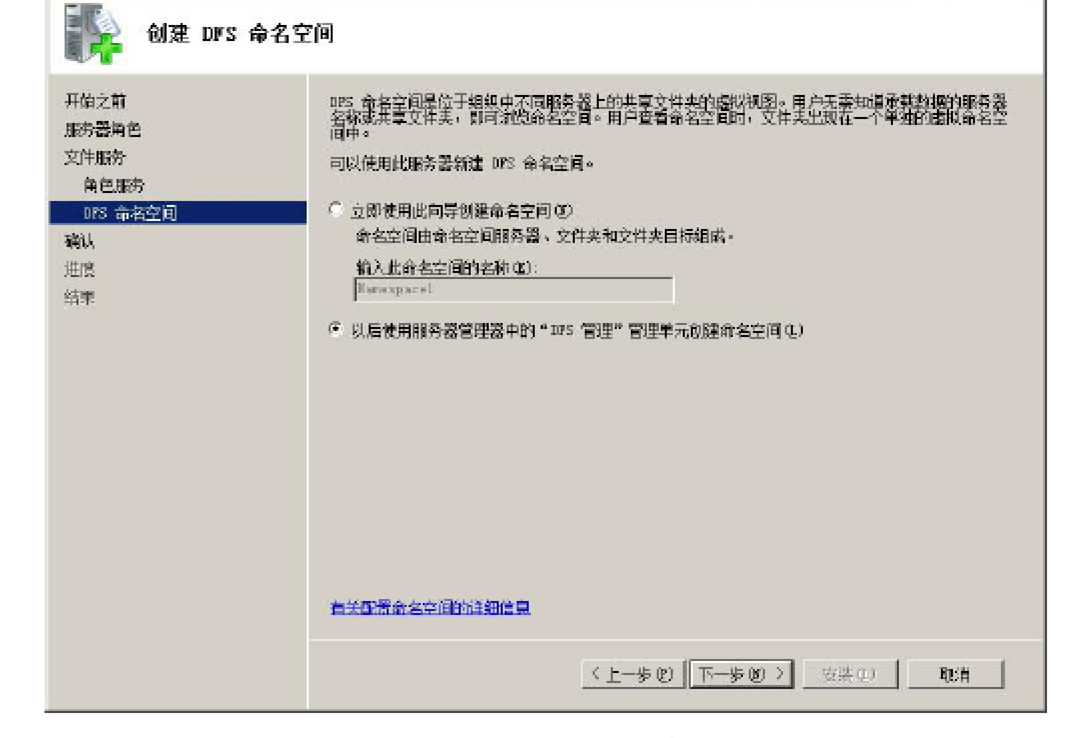


图 10-4　创建 DFS 命名空间

05 在“确认安装选择”对话框中，可以查看即将安装的角色服务及功能，如图 10-5 所示。

06 单击“安装”按钮开始安装。安装完成后，显示“安装结果”对话框，单击“关闭”按钮退出，如图 10-6 所示。

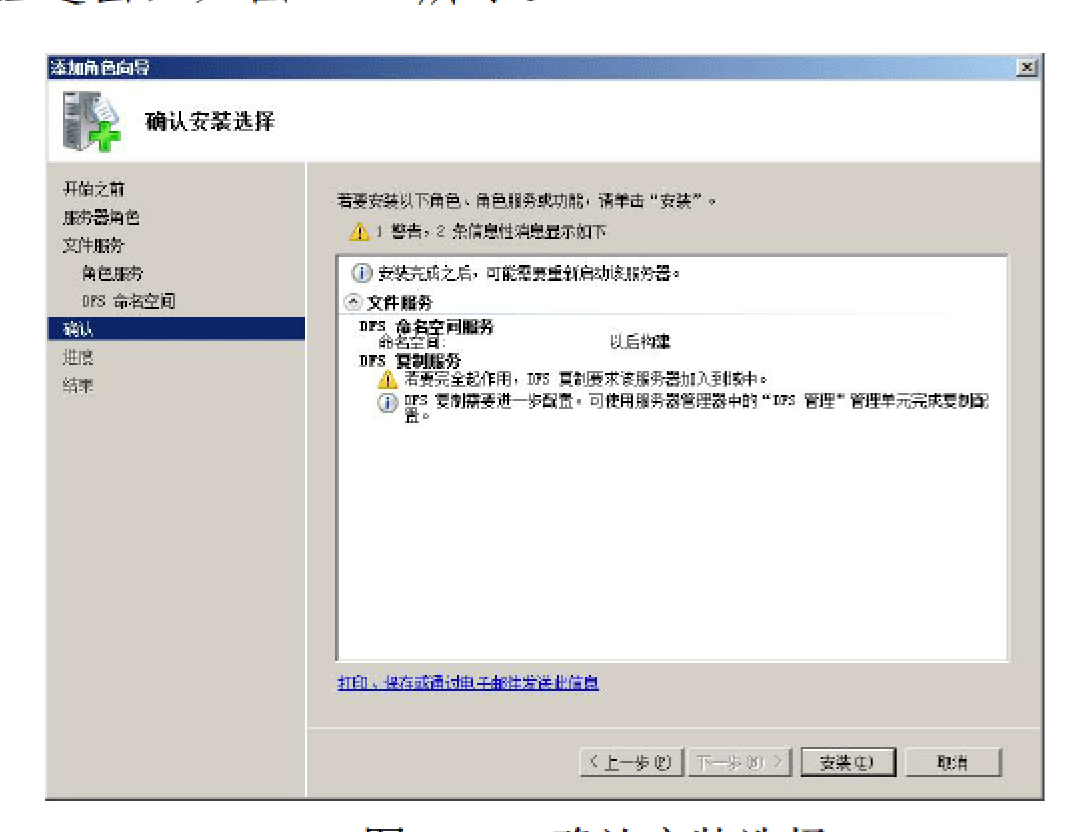


图 10-5　确认安装选择



图 10-6　安装结果

10.2　创建和管理命名空间（DFS 的使用）

使用 DFS 命名空间，可以将位于不同服务器上的共享文件夹组合到一个或多个逻辑结构的命名空间。每个命名空间作为具有一系列子文件夹的单个共享文件夹显示给用户。但是，命名空间的基本结构可以包含位于不同服务器以及多个站点中的大量共享文件夹。命名空间提高了可用性，并在可用时自动将用户连接到同一活动目录域服务（AD DS）站点中的共享文件夹，而不是通过广域网（WAN）连接对其进行路由。

10.2.1　创建命名空间

创建命名空间的步骤如下。

01 选择“开始”→“管理工具”→“DFS Management”菜单，打开“DFS 管理”窗口，如图 10-7 所示。

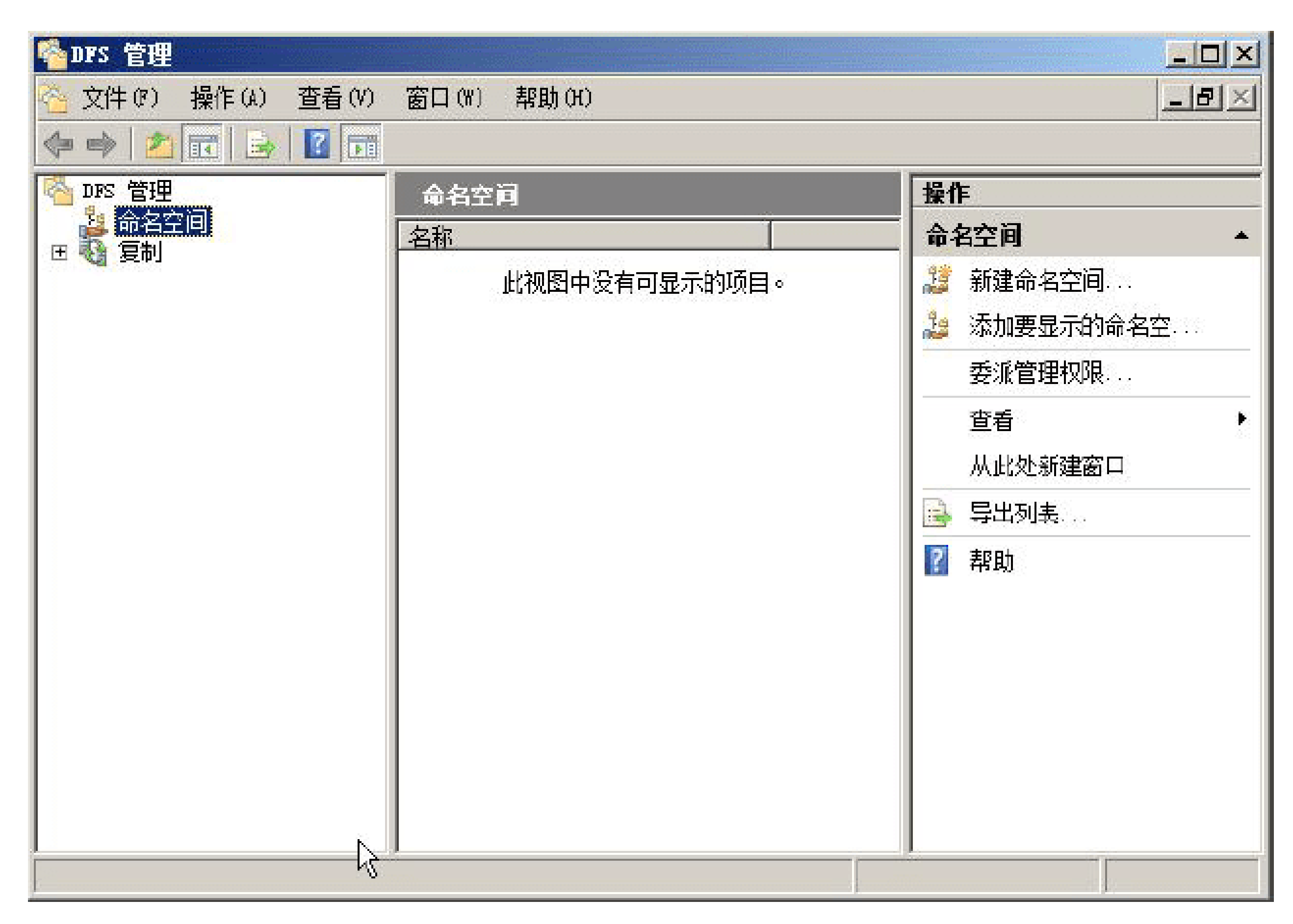
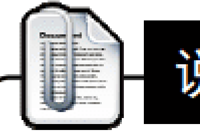


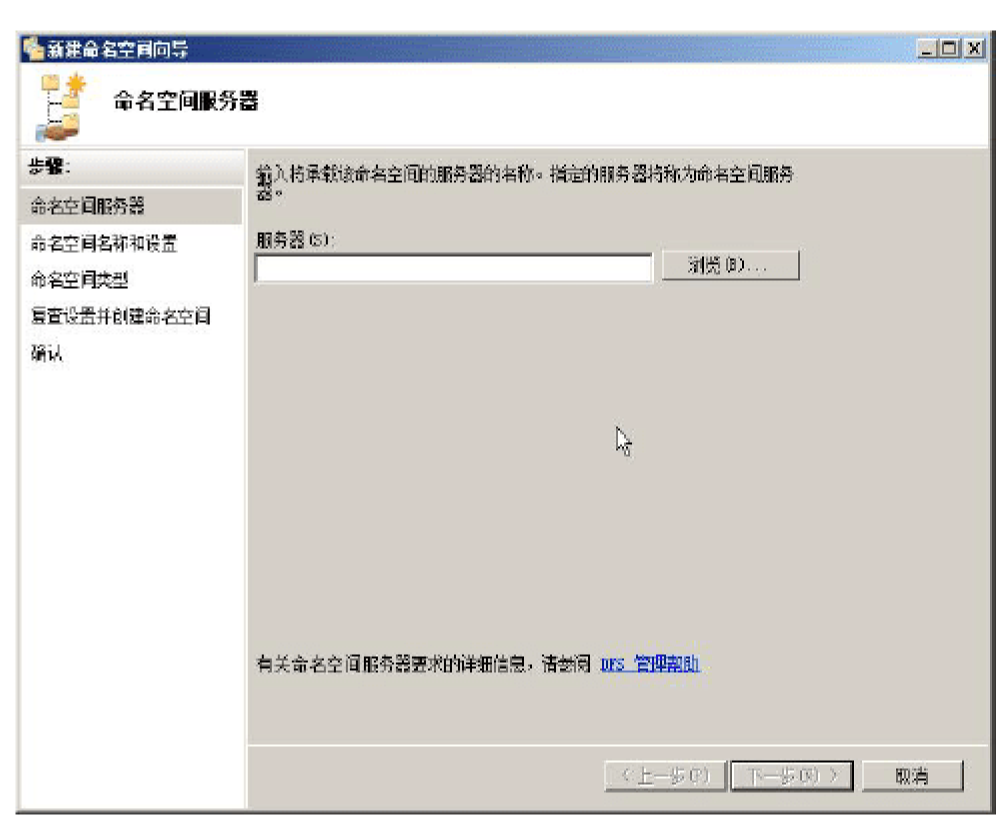
图 10-7　DFS 管理

02 从“DFS 管理”窗口中，用鼠标右键单击“命名空间”，从快捷菜单中选择“新建命名空间”命令，运行“新建命名空间向导”，如图 10-8 所示。单击“浏览”按钮，打开“选择计算机”对话框，单击“高级”按钮，然后单击“立即查找”按钮，选择“WIN2008SER”，如图 10-9 所示。单击“确定”按钮返回。



说 明

也可以在“服务器名称”文本框中直接输入计算机名称，本例中为“WIN2008SER”，然后单击“确定”按钮，返回“命名空间服务器”对话框。



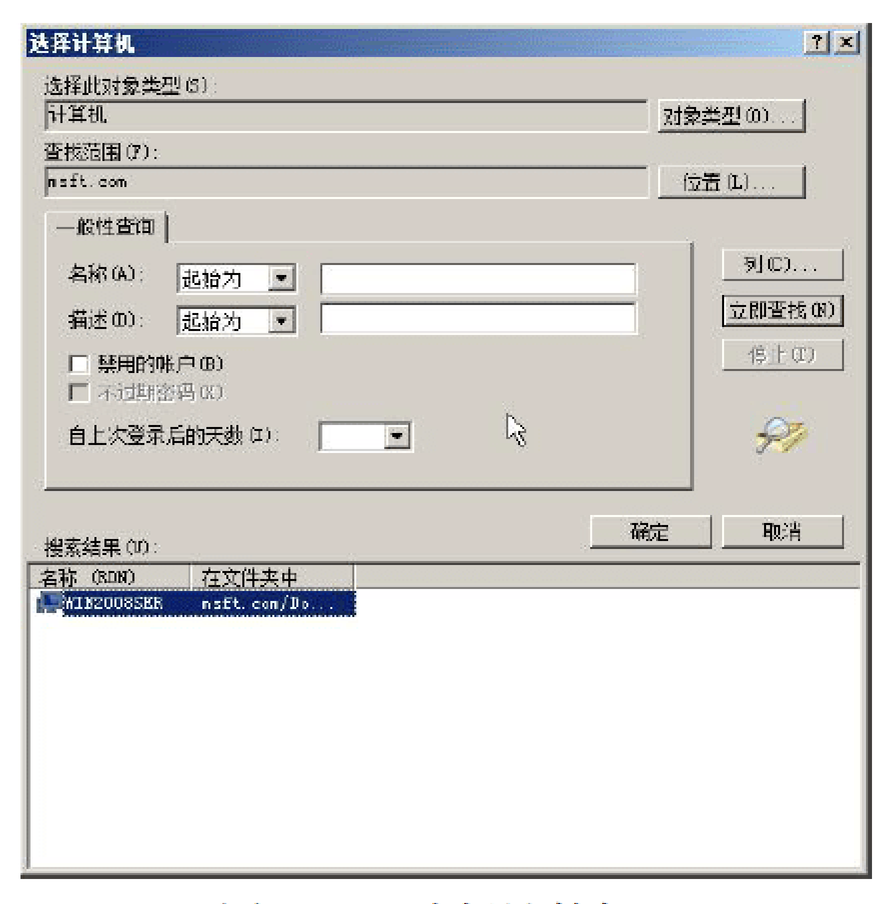


图 10-8　新建命名空间向导　　　　图 10-9　选择计算机

03 打开“命名空间名称和设置”对话框，在“名称”文本框中输入命名空间的名称，通常选择一个比较简短、易记的名称，本例中为“dfs-root”，如图 10-10 所示。

04 单击“编辑设置”按钮，打开“编辑设置”对话框，在“共享文件夹的本地路径”文本

框中使用默认路径，选择“Administrator 具有完全访问权限；其他用户具有只读权限”单选按钮，如图 10-11 所示，单击“确定”按钮。

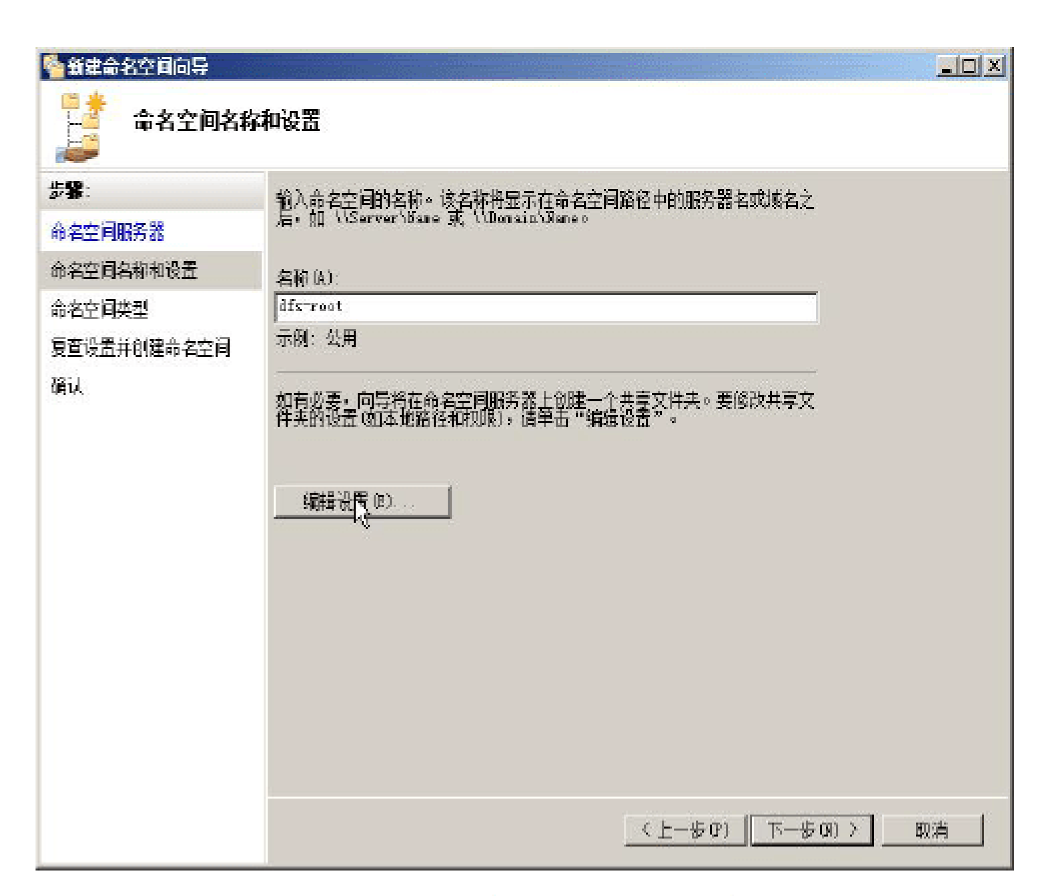


图 10-10 命名空间名称和设置



图 10-11 编辑设置

05 返回到“命名空间名称和设置”对话框后单击“下一步”按钮，打开“命名空间类型”对话框，选中“基于域的命名空间”单选按钮，如图 10-12 所示。

06 在“复查设置并创建命名空间”对话框，查看设置，如图 10-13 所示。然后单击“创建”按钮。



图 10-12 命名空间类型



图 10-13 复查设置

07 显示“确认”对话框，如图 10-14 所示。单击“关闭”按钮，返回到“DFS 管理”窗口，如图 10-15 所示。

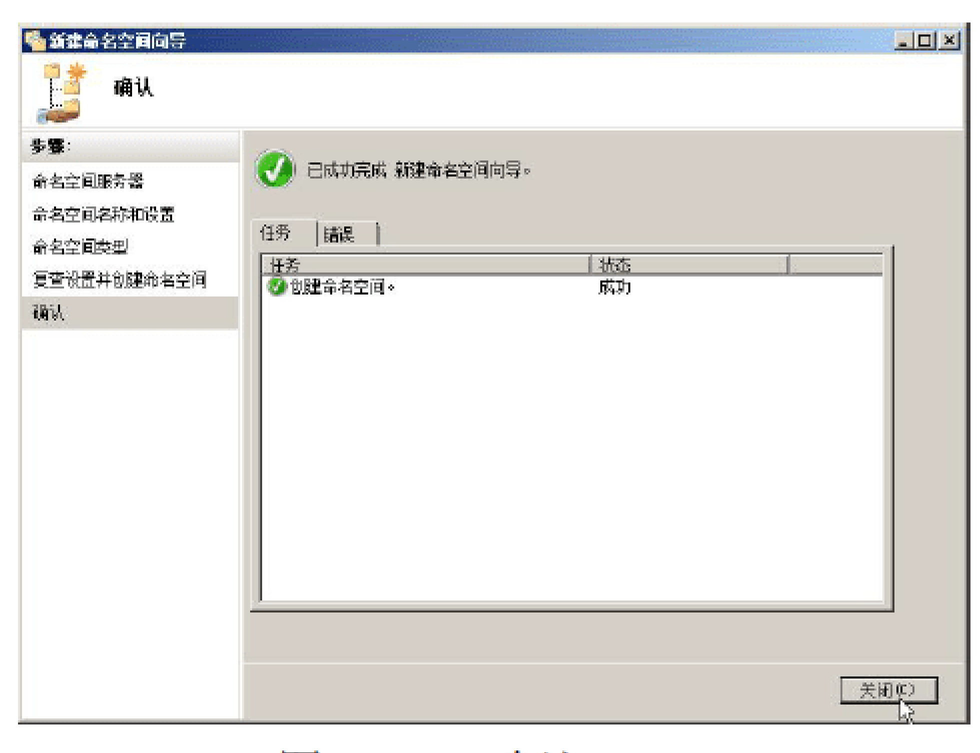


图 10-14 确认

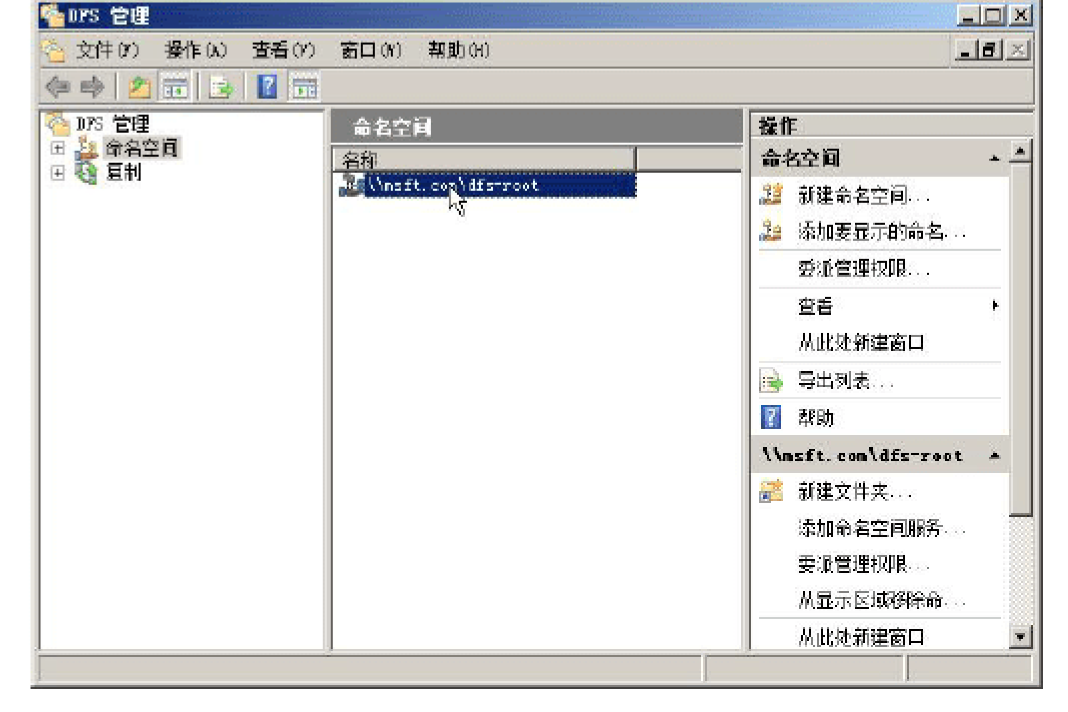


图 10-15 DFS 管理

10.2.2 在命名空间中创建文件夹

在创建命名空间后，可以将各服务器中创建的共享文件夹添加到命名空间中统一管理和使用，而其他用户再访问各服务器提供的共享资源时，只需要统一访问 DFS 命名空间即可。在此可以看到，所谓 DFS 命名空间，只不过是把需要共享的资源进行统一管理而已。

在本小节的操作中，将把 WIN2008SER 服务器提供的 soft 共享、fs2 提供的 vod-fs2 共享添加到 DFS 命名空间中，步骤如下。

01 在“DFS 管理”窗口中展开“命名空间”选项，右击已创建的命名空间，选择快捷菜单中的“新建文件夹”命令，显示“新建文件夹”对话框，如图 10-16 所示。首先添加 WIN2008SER 提供的 soft 共享文件夹。在“名称”文本框中输入文件夹名，这个文件夹名是在 DFS 命名空间中访问提供的共享的快捷名称，在本例中为“software”。



图 10-16 新建文件夹

02 在图 10-16 中单击“添加”按钮，显示“添加文件夹目标”对话框，如图 10-17 所示。

03 单击“浏览”按钮，打开“浏览共享文件夹”对话框，单击“浏览”按钮，打开“选择计算机”对话框，输入计算机名称，本例为“WIN2008SER”。单击“确定”按钮返回，从“共享文件夹”列表中选择“soft”文件夹，如图 10-18 所示。然后单击“确定”按钮。



图 10-17　添加文件夹目标　　　图 10-18　浏览共享文件夹

04 显示“添加文件夹目标”对话框，显示添加的目标路径，如图 10-19 所示。然后单击“确定”按钮。

05 在“文件夹目标”文本框中将显示已添加的文件夹路径，本例中为“\\WIN2008SER\soft”，如图 10-20 所示。单击“确定”按钮，添加文件夹目标完成。



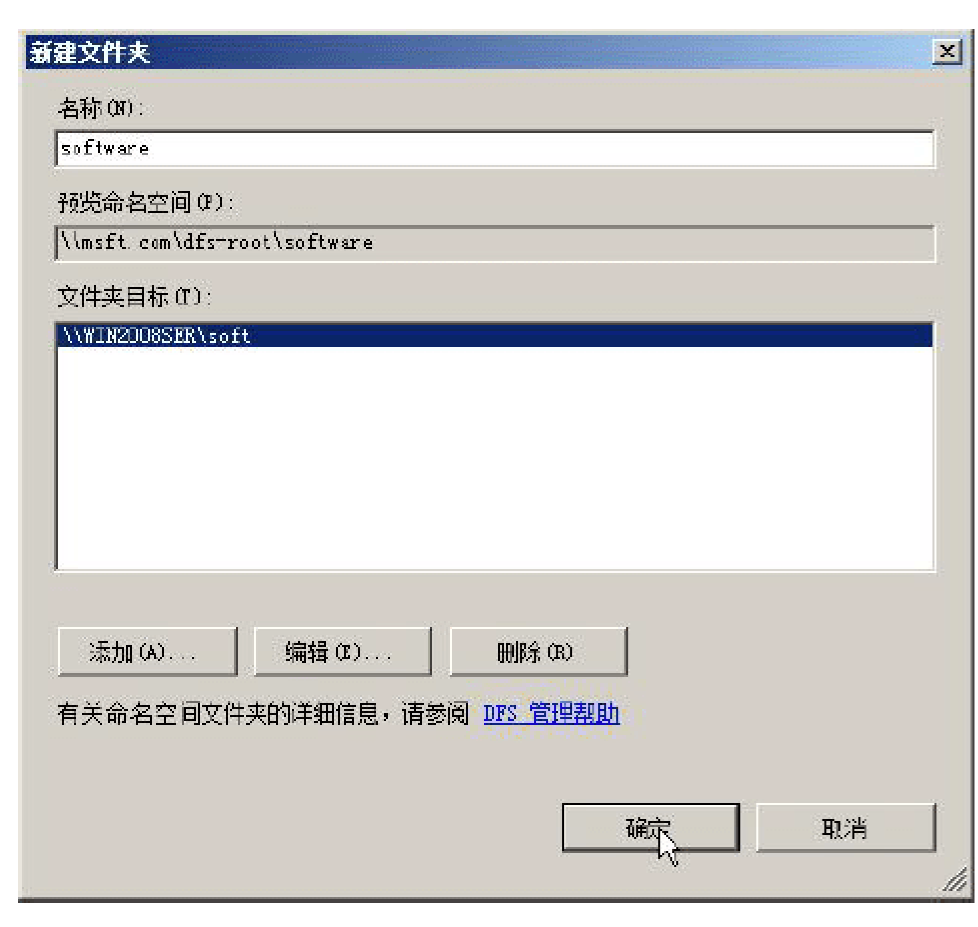


图 10-19　添加文件夹目标　　　图 10-20　已添加的文件夹路径

06 参照上述步骤，可继续添加名为 vod 的文件夹到 fs2 服务器的 vod-fs2 共享

10.2.3　配置文件共享

“共享和存储管理”为用户提供了一个用于管理共享资源（如文件夹和卷）以及存储资源的集中位置，它提供了一个管理两种重要服务器资源的集中位置：在网络上共享的文件夹和卷以及磁盘和存储子系统中的卷。

下面介绍一下利用“共享和存储管理”控制台设置共享的方法，具体步骤如下。

01 选择“开始”→“管理工具”→“共享和存储管理”，打开“共享和存储管理”控制台，如图 10-21 所示。

02 右击控制台左侧的“共享和存储管理（本地）”选项，在快捷菜单中选择“设置共享”选项，运行“设置共享文件夹向导”。在“共享文件夹位置”对话框中，单击“浏览”按钮，选择要设置为共享的文件夹，本例中为 D 盘下的 software 文件夹，如图 10-22 所示。



图 10-21　共享和存储管理

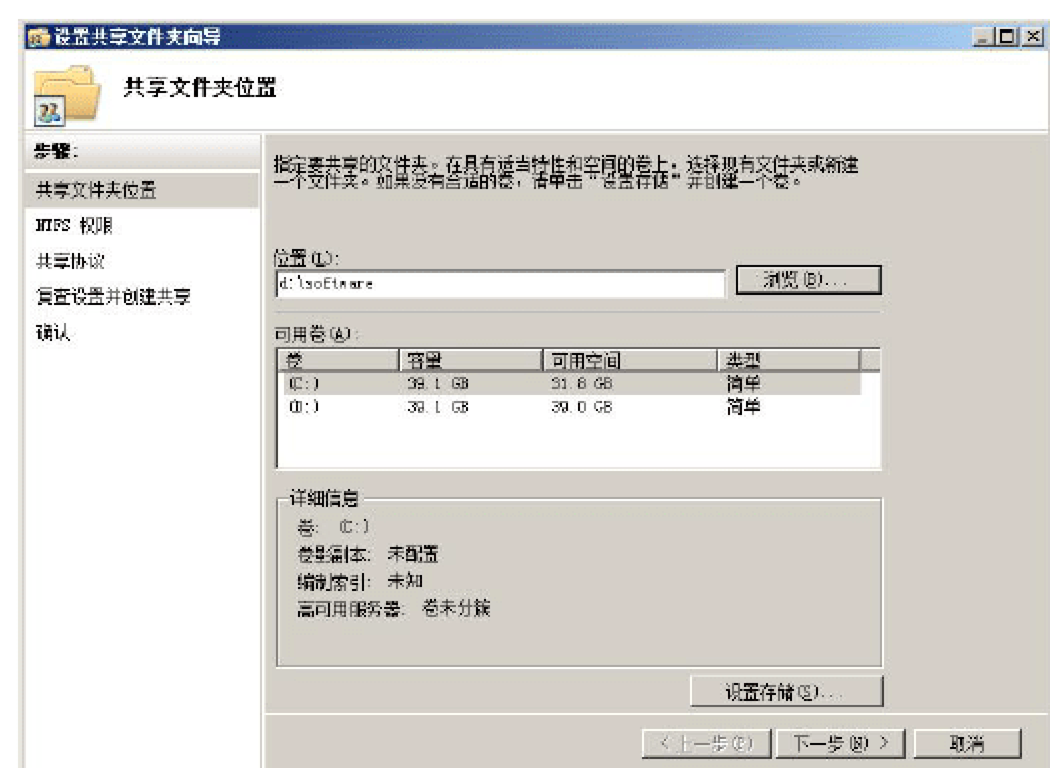


图 10-22　设置共享文件夹向导

03 在“NTFS 权限”对话框中，选择“否，不更改 NTFS 权限”单选按钮（若用户需要更改共享文件夹的 NTFS 权限，也可以选择“是，更改 NTFS 权限”选项），如图 10-23 所示。

04 在“共享协议”对话框，选中“SMB”复选框，可以设置共享名，也可使用默认值，如图 10-24 所示。若服务器上安装了网络文件系统（NFS）服务，还可以为共享资源指定基于 NFS 的访问权限。




图 10-23　NTFS 权限

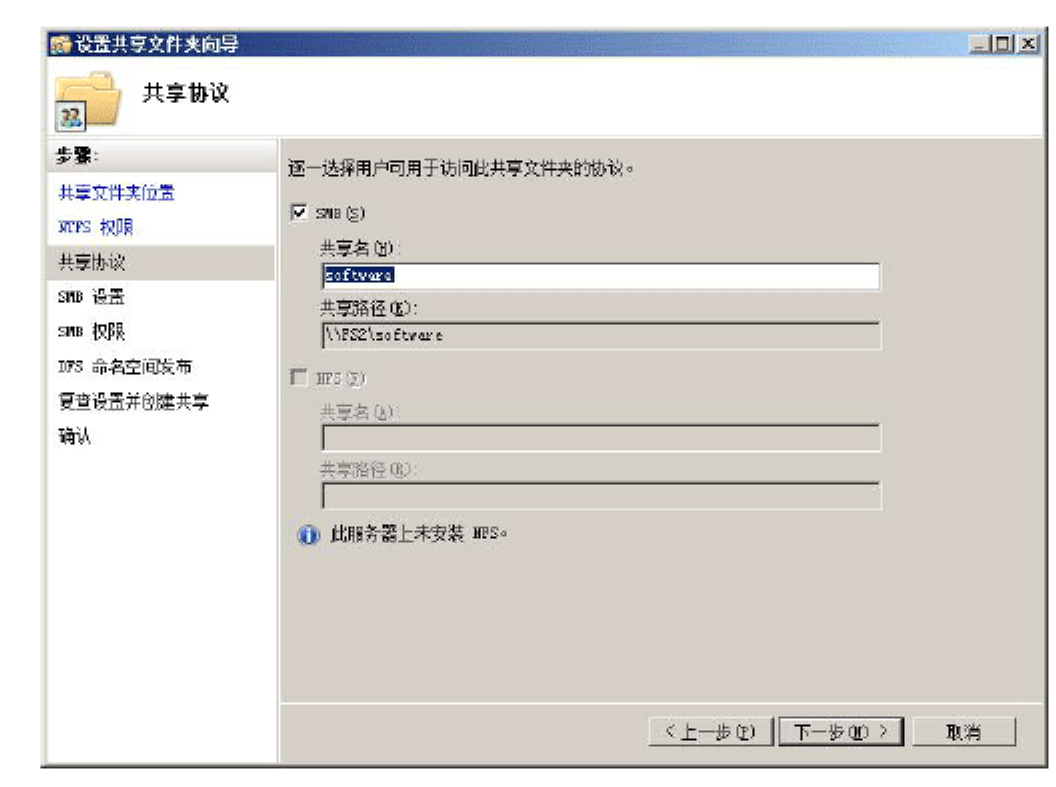


图 10-24　共享协议

05 在“SMB 设置”对话框，单击“高级”按钮可以更改相应设置，如图 10-25 所示。

06 在显示“SMB 权限”对话框，选择“Administrator 具有完全控制权限；所有其他用户和组只有读取访问权限”单选按钮，如图 10-26 所示

07 在“DFS 命名空间发布”对话框中，若需要将此 SMB 共享发布到 DFS 命名空间中，可以选中“将此 SMB 共享发布到 DFS 命名空间”复选框，在“命名空间中的父文件夹：”文本框中输入“\\msft.com\dfs-root”，在“新文件夹名称”文本框中输入共享的名称，如“software-fs2”，如图 10-27 所示。

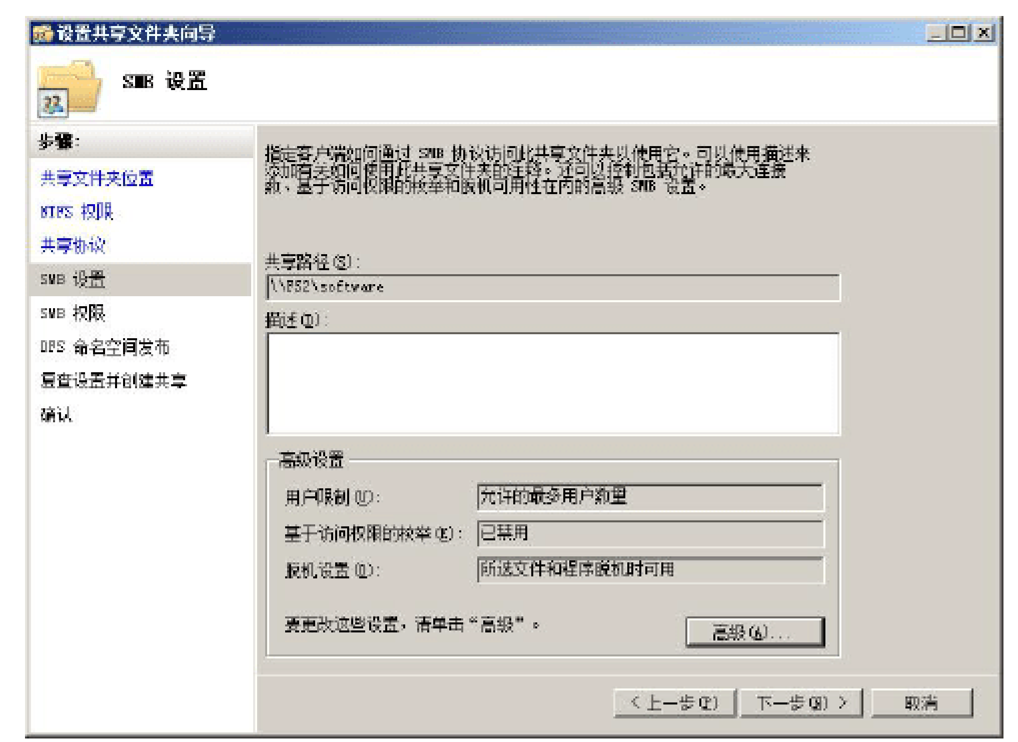


图 10-25　SMB 设置



图 10-26　SMB 权限

08 在“复查设置并创建共享”对话框，可以看到将要设置的共享文件夹的详细信息，如图 10-28 所示。单击“创建”按钮，创建共享完成。然后在“确认”对话框中，单击“关闭”按钮即可。

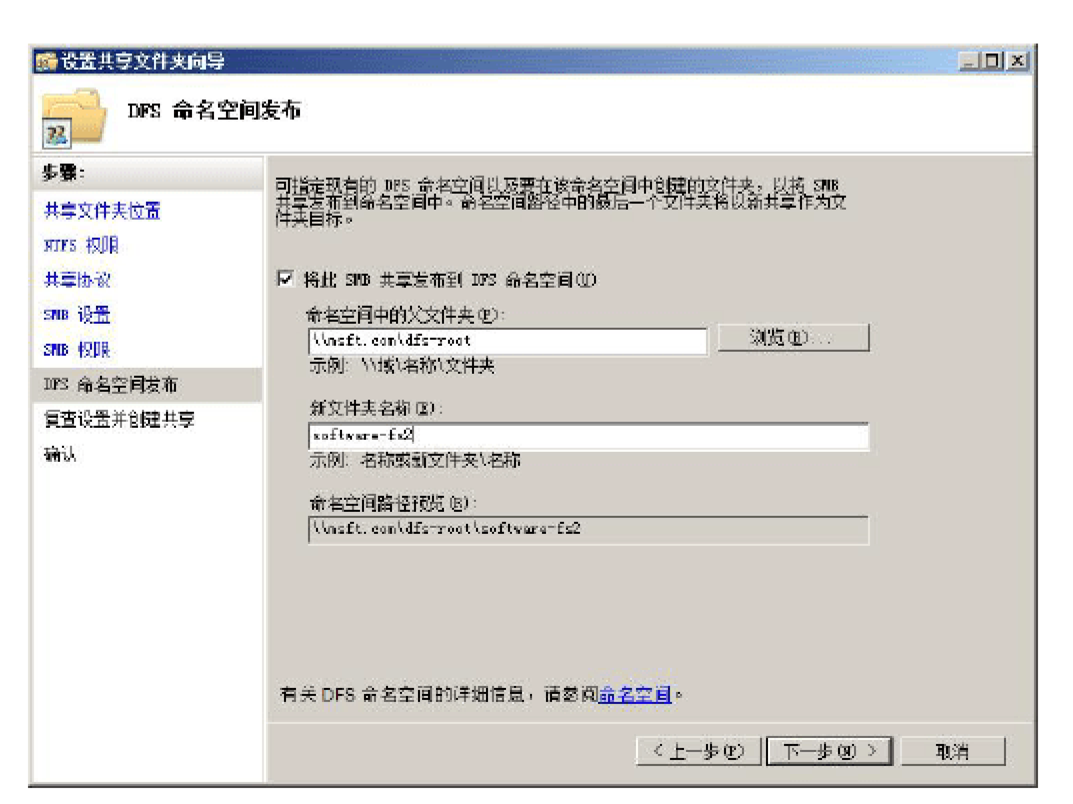


图 10-27　DFS 命名空间发布

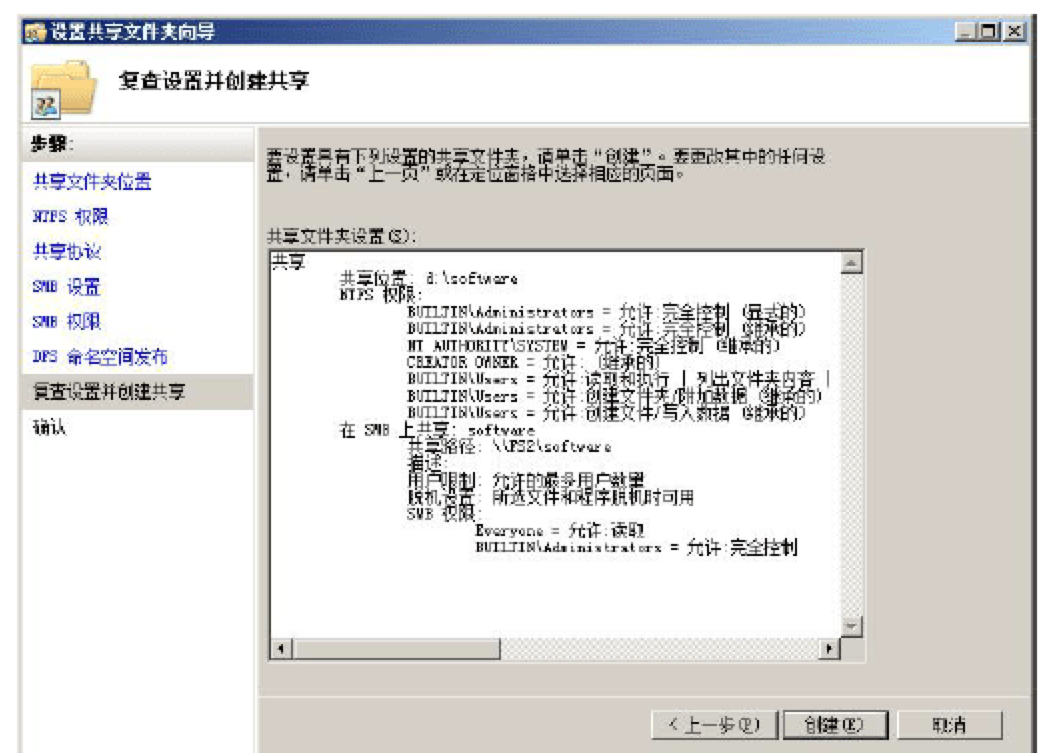


图 10-28　复查设置并创建共享

09 在“共享和存储管理”控制台中，可以看到已设置的共享，如图 10-29 所示。

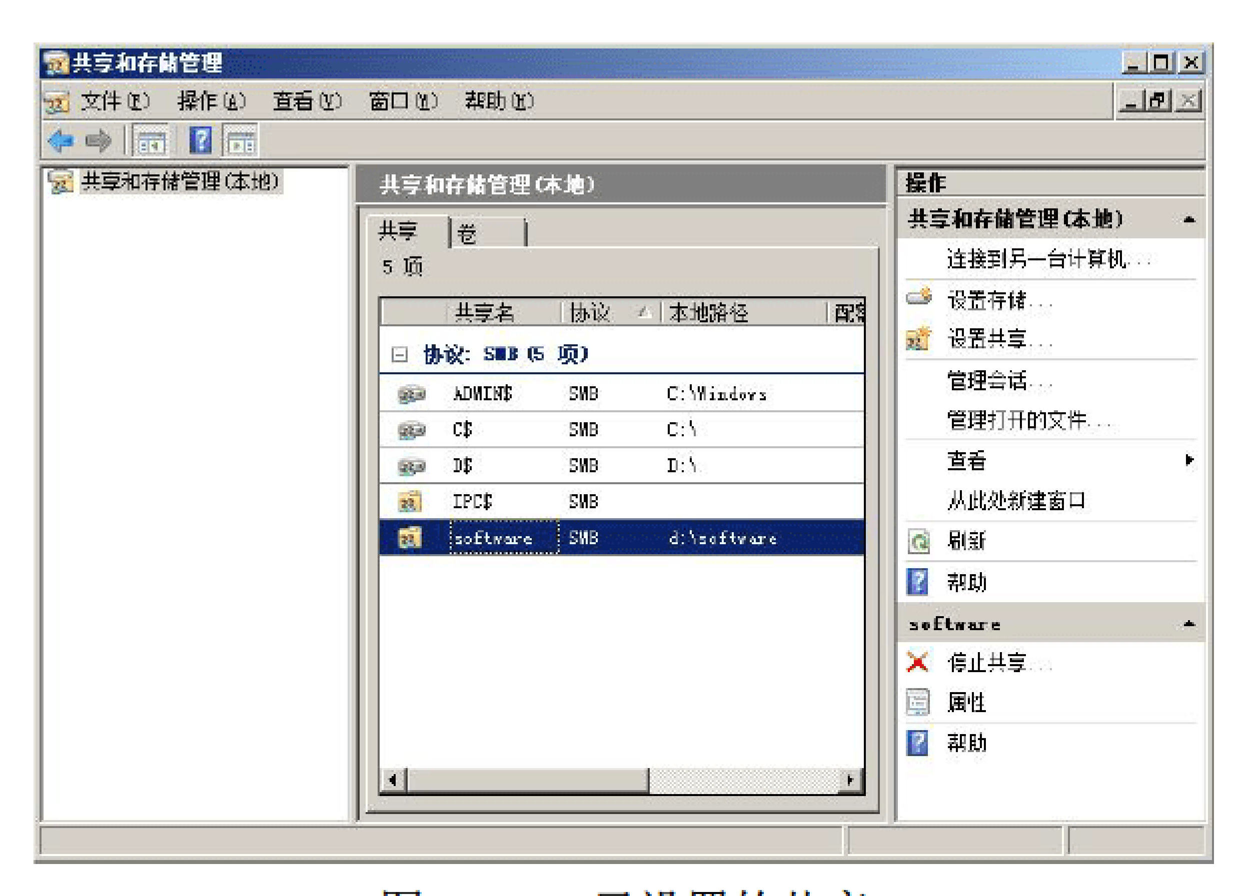


图 10-29　已设置的共享

10.3　管理 DFS 复制

DFS 复制是从 Windows 2000 Server 开始引入的文件复制服务（FRS），是一个基于状态的新型多主机复制引擎，支持复制计划和带宽限制。DFS 复制使用一种称为远程差分压缩（RDC）的新的压缩算法。RDC 是一种“线上差分”客户端/服务器协议，可用于在有限带宽网络上有效地更新文件。RDC 检测文件中数据的插入、删除和重新排列，使“DFS 复制”能够在文件更新时仅复制已更改的文件块。

10.3.1　DFS 复制简介

DFS 复制是一种有效的多主机复制引擎，可用于保持跨有限带宽网络连接的服务器之间的文件夹同步。它将文件复制服务（FRS）替换为用于 DFS 命名空间，以及用于复制使用 Windows Server 2008 域功能级别的、域中的 Active Directory 域服务（AD DS）SYSVOL 文件夹的复制引擎。

DFS 复制使用许多复杂的进程来保持多个服务器上的数据同步，在一个成员上进行的任何更改均将复制到复制组的所有其他成员上。DFS 复制通过监视更新序列号（USN）日志来检测卷上的更改，DFS 复制仅在文件关闭后复制更改。

在发送或接收文件之前，DFS 复制使用暂存文件夹来暂存文件。DFS 复制使用版本矢量交换协议来确定需要同步的文件。该协议通过网络为每个文件发送不到 1KB 的数据，用于同步发送成员和接收成员上与已更改文件关联的元数据。

文件更改后，只会复制已更改的文件块，而不会复制整个文件。RDC 协议确定已更改的文件块。使用默认的设置，RDC 适用于任何大于 64KB 的文件类型，仅通过网络传输文件的一小部分。

DFS 复制对冲突的文件（即在多个服务器上同时更新的文件）使用最后写入者优先的冲突解决启发方式，对名称冲突使用最早创建者优先的冲突解决启发方式。解决冲突失败的文件和文件夹移至一个称为冲突和已删除文件夹的文件夹。还可以通过配置该服务，将已删除文件复制到冲突和已删除文件夹，以便在文件或文件夹被删除后进行检索。

DFS 复制可以自我修复，可以自动从 USN 日志覆盖、USN 日志丢失或 DFS 复制数据库丢失中恢复。DFS 复制使用 Windows 管理规范（Windows Management Instrumentation，WMI）提供的程序，为获取配置和监视来自 DFS 复制服务的信息提供接口。

10.3.2　DFS 复制要求

DFS 复制具有以下要求：

- 扩展（或更新）Active Directory 域服务（AD DS）架构以包括 Windows Server 2003 R2 或 Windows Server 2008 架构附加功能。有关扩展 AD DS 架构的信息，可访问 Microsoft 网站（http://go.microsoft.com/fwlink/?LinkId=93051）
- 验证复制组的所有成员运行的是否是 Windows Server 2008 或 Windows Server 2003 R2。
- 在充当复制组成员的所有服务器上，安装具有 DFS 复制角色服务的文件服务角色。
- 在服务器上安装“DFS 管理”管理单元以管理复制。此服务器无法运行 Windows Server 2008

操作系统的服务器核心安装。

- 检查您的防病毒软件是否与 DFS 复制兼容。
- 确保复制组中的所有服务器位于同一林中，不能跨不同林中的服务器进行复制。
- 将已复制文件夹存储在 NTFS 卷上。
- 在节点的本地存储中查找故障转移群集的已复制文件夹。DFS 复制服务未设计为与群集组件协调，并且该服务不会将故障转移到另一个节点。

部署 DFS 复制时不要超过以下限制：

- 每个服务器最多可以是 256 个复制组的成员。
- 每个复制组最多可以包含 256 个已复制文件夹。
- 每个服务器最多可以具有 256 个连接（例如 128 个传入连接和 128 个传出连接）。
- 在每个服务器上，复制组数乘以已复制文件夹数再乘以连接数，结果必须等于或小于 1024。
- 一个复制组最多可以包含 256 个成员。
- 一个卷最多可以包含 800 万个已复制文件夹，一个服务器最多可以包含 1TB 的已复制文件。

10.3.3　创建 DFS 复制组

要使用 DFS 复制发布数据，需要创建一个复制组，然后选择包含一个或两个中心服务器（用于冗余）的集散拓扑。创建 DFS 复制组的具体步骤如下。

01 在“DFS 管理”窗口中，选择“复制”项，右击并选择快捷菜单中的“新建复制组”选项，运行“新建复制组向导”。在“复制组类型”对话框中，选择“多用途复制组”单选按钮，如图 10-30 所示。

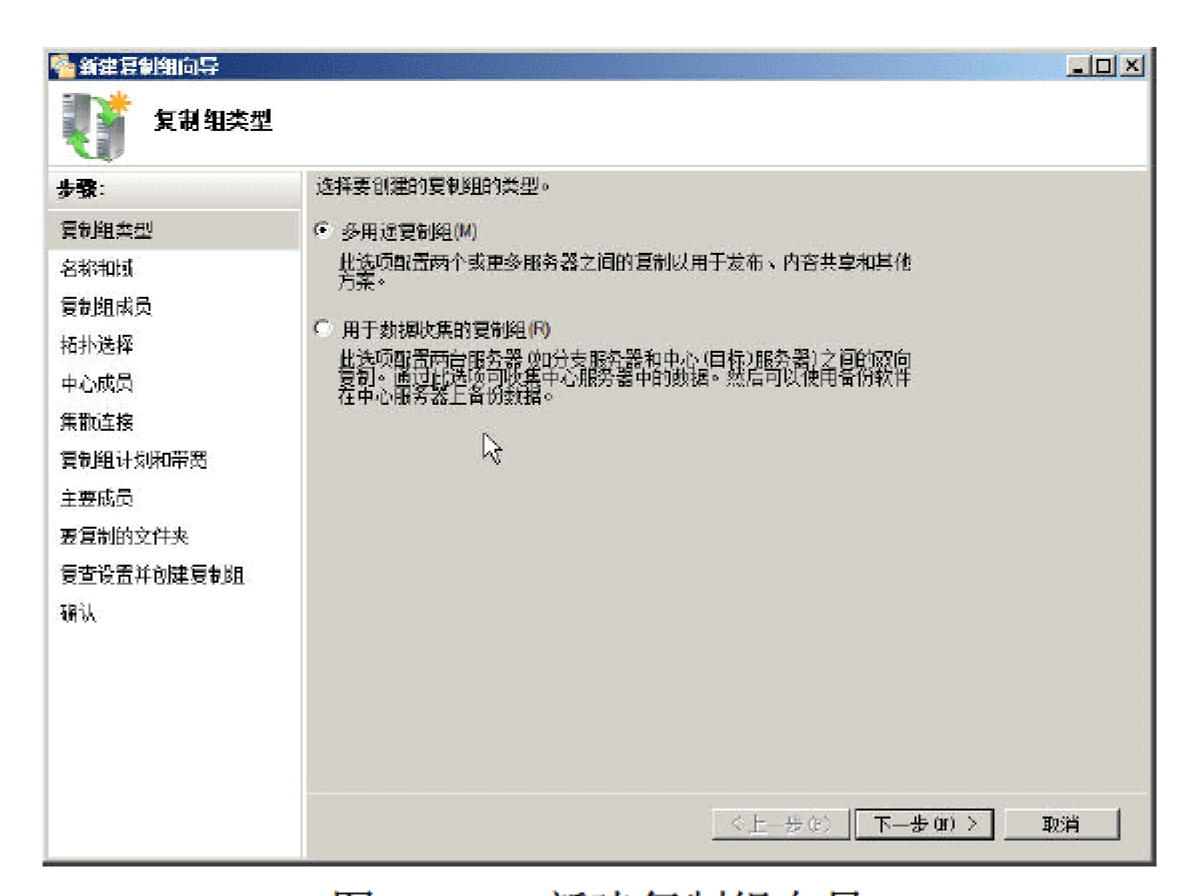


图 10-30　新建复制组向导

02 在“名称和域”对话框中，在“复制组的名称”文本框中输入有代表意义的复制组名，如“PUB-SOFT-DFS”，如图 10-31 所示。

03 在“复制组成员”对话框中，单击“添加”按钮，选择要添加的服务器，本例中为“WIN2008SER”和“FS2”，如图 10-32 所示。



图 10-31　名称和域

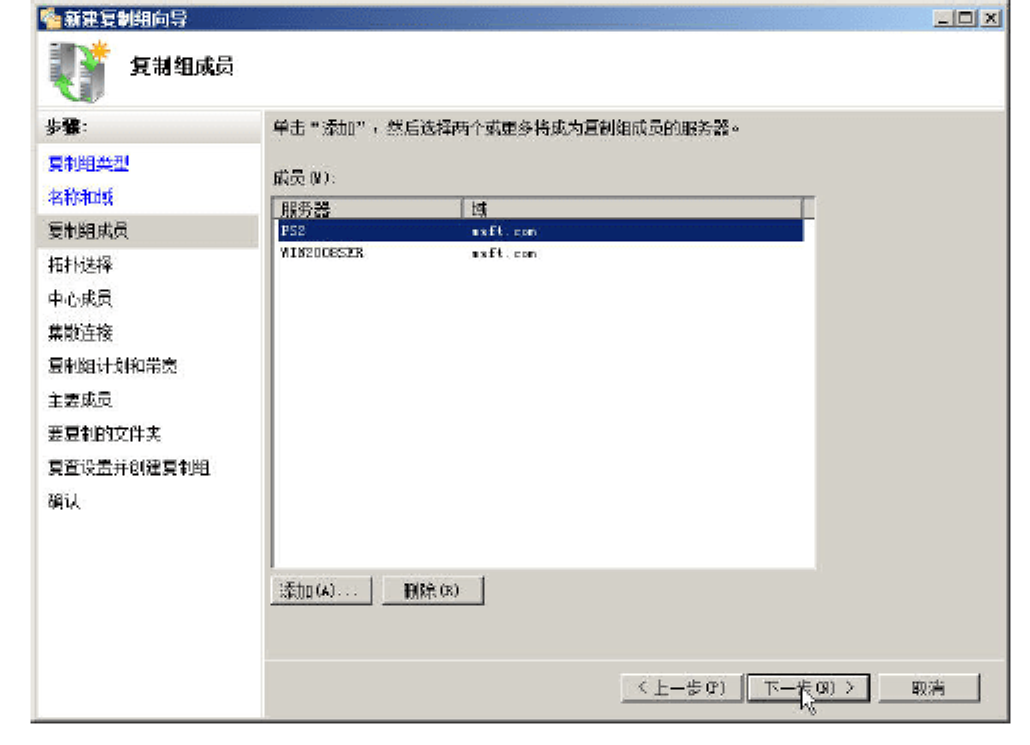


图 10-32　复制组成员

04 在“拓扑选择”对话框中，选择“交错”单选按钮，如图 10-33 所示。

05 在“复制组计划和带宽”对话框，选择“使用指定带宽连续复制”单选按钮，在“带宽”下拉列表框中选择“完整”选项，如图 10-34 所示。



图 10-33　拓扑选择

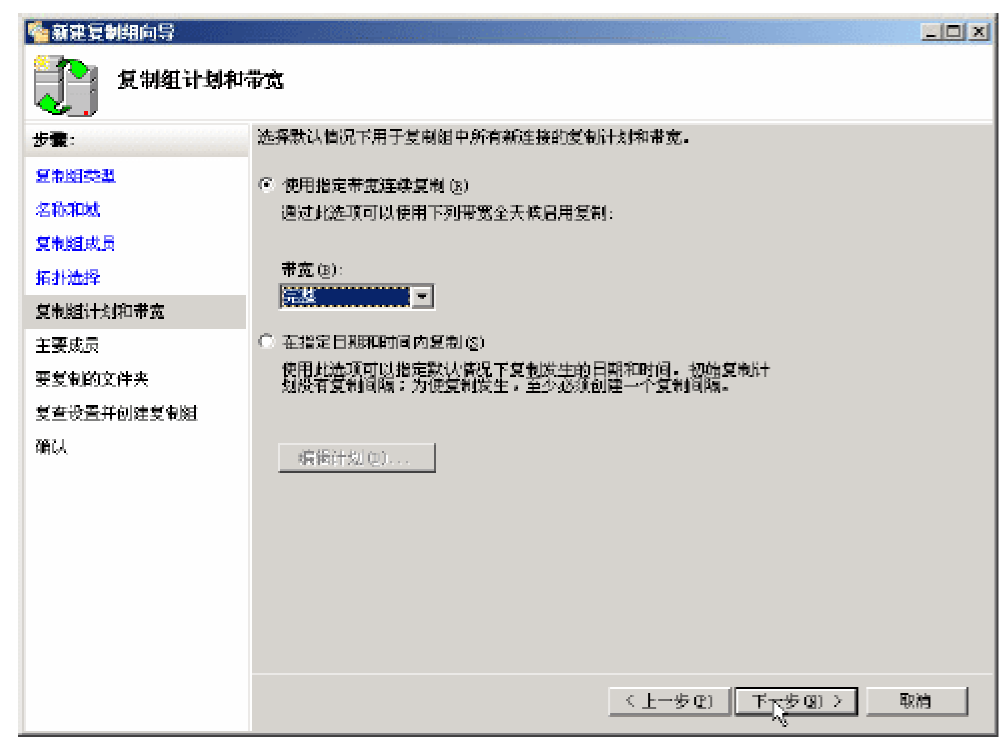


图 10-34　复制组计划和带宽

06 在“主要成员”对话框中，在“主要成员”下拉列表中选择“WIN2008SER”，如图 10-35 所示。

07 在“要复制的文件夹”对话框（如图 10-36 所示）中，单击“添加”按钮，显示“添加要复制的文件夹”对话框，如图 10-37 所示。

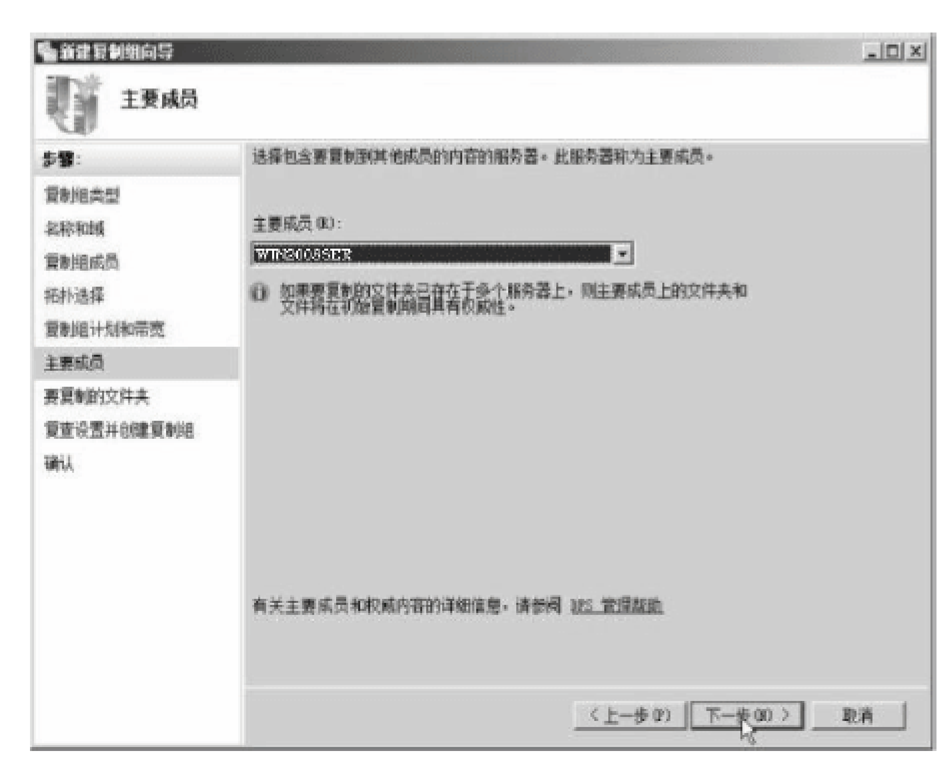


图 10-35　主要成员

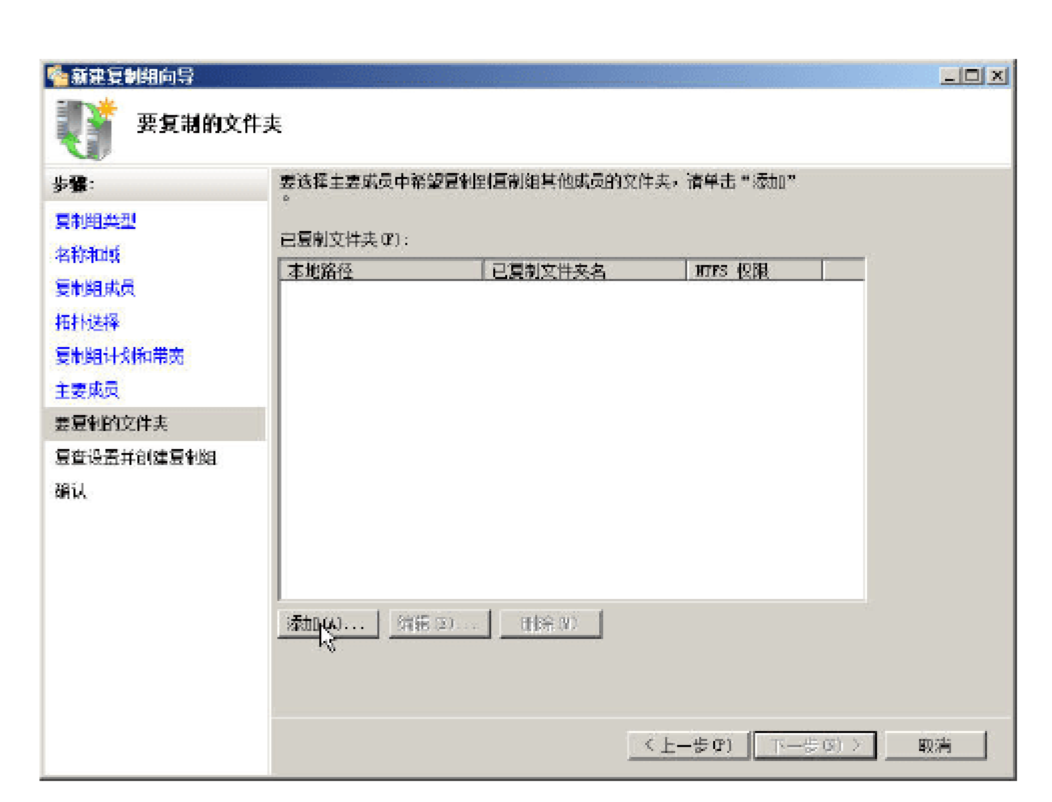


图 10-36　启用成员身份状态

08 在“要复制的文件夹的本地路径”文本框中输入或浏览到所要复制的路径，本例中使用“D:\PUB-SOFT-DFS”，如图 10-37 所示。

09 单击“确定”按钮返回，由于其他成员的本地路径为“已禁用”，应单击“编辑”按钮，设置路径，将“成员身份状态”设置为“已启用”，如图 10-38 所示。

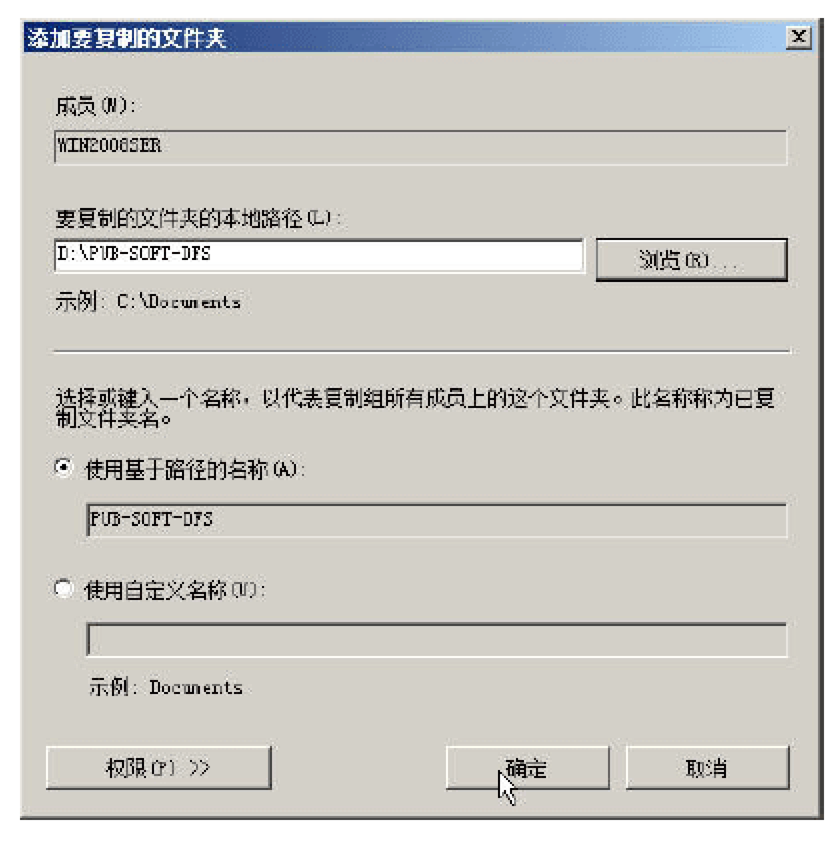


图 10-37 添加要复制的文件夹

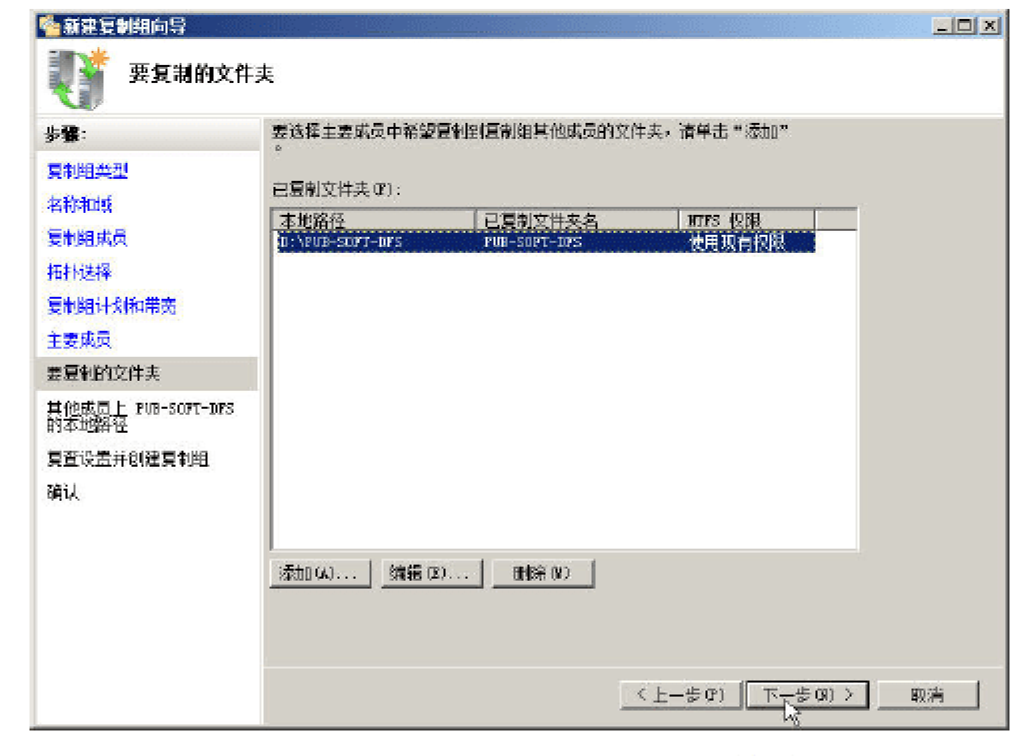


图 10-38 要复制的文件夹

10 在“复查设置并创建复制组”对话框，单击“创建”按钮，显示“确认”对话框，如图 10-39 所示。

11 单击“关闭”按钮，复制组创建完成，如图 10-40 所示。

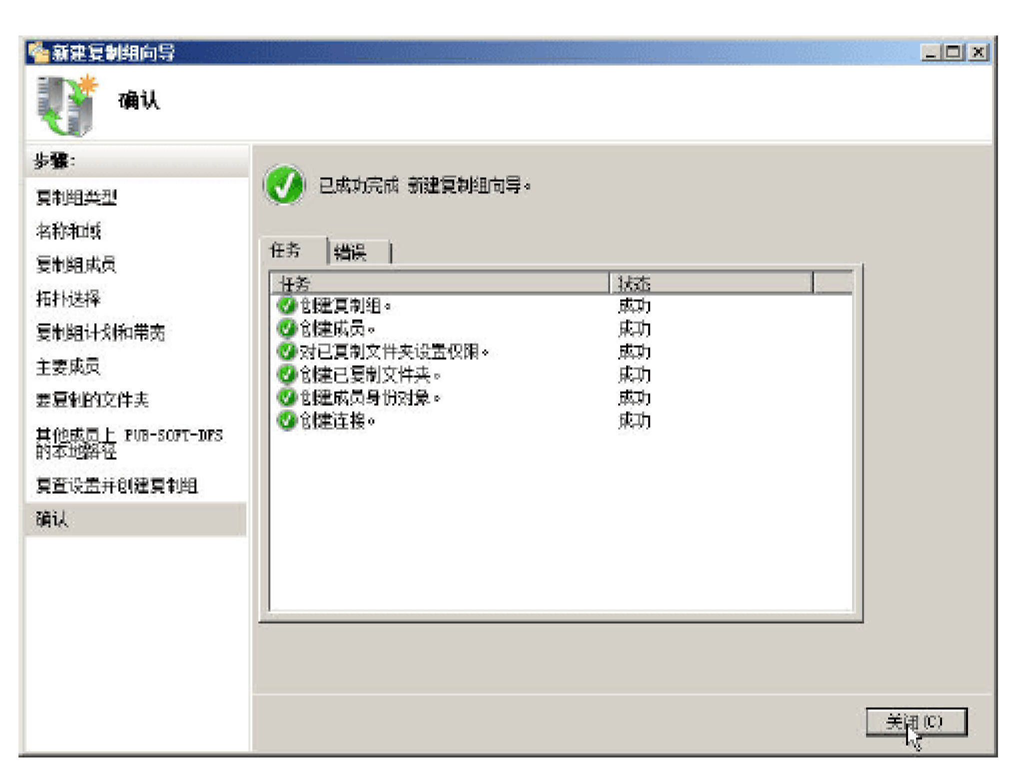


图 10-39 确认

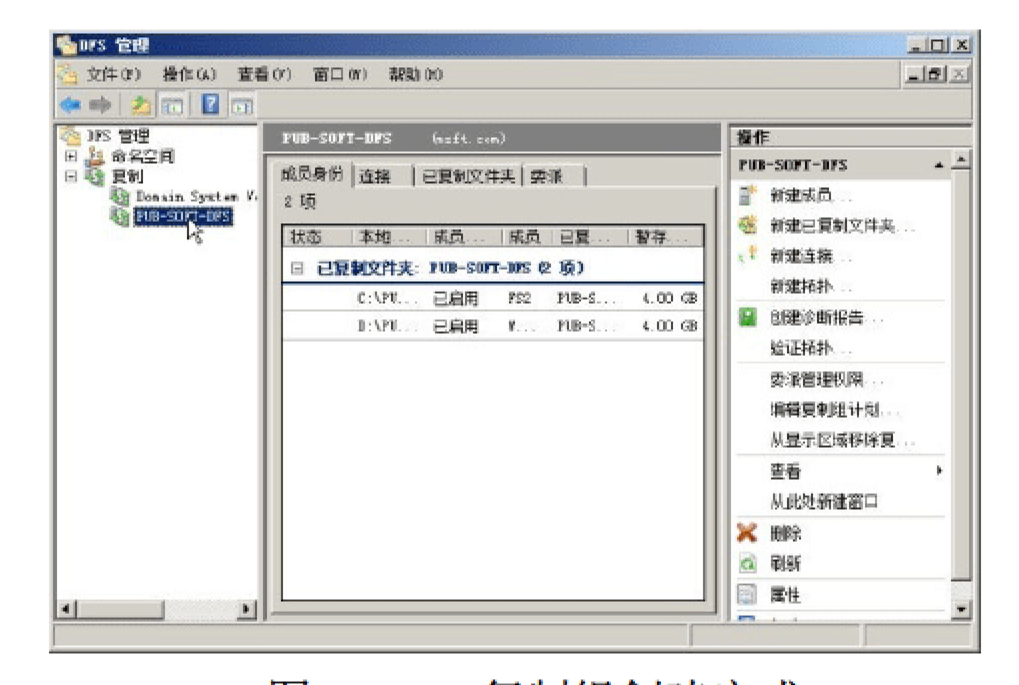


图 10-40 复制组创建完成

10.3.4 发布 DFS 复制组

复制组创建完成以后，需要将“已复制的文件夹”发布，具体步骤如下。

01 选中要发布的复制组，并单击“已复制文件夹”选项卡，如图 10-41 所示。

02 右键单击要共享的已复制文件夹，在快捷菜单中选择“在命名空间中共享和发布”命令，显示“共享和发布已复制文件夹向导”。选择“共享和发布命名空间中的已复制文件夹”单选按钮，如图 10-42 所示。

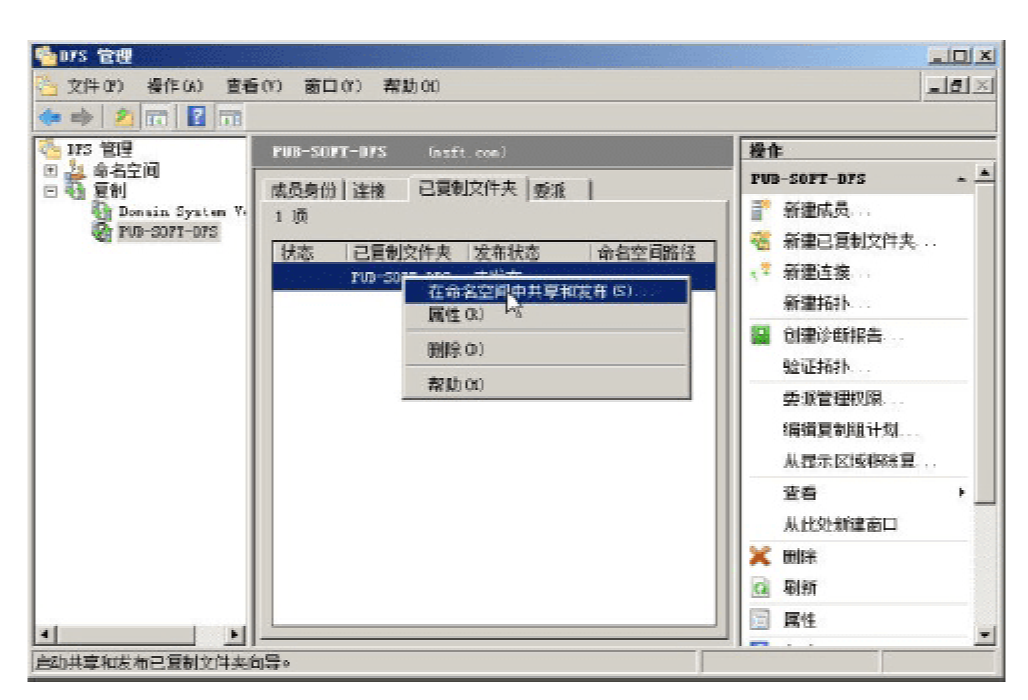



图 10-41　已复制文件夹



图 10-42　共享和发布已复制文件夹向导

03 在图 10-42 中单击“下一步”按钮，显示“共享已复制文件夹”对话框，如图 10-43 所示。

04 在图 10-43 中单击“下一步”按钮，打开“命名空间路径”对话框，在“命名空间中的父文件夹”文本框中选择路径，本例为“\\msft.com\dfs-root”，如图 10-44 所示

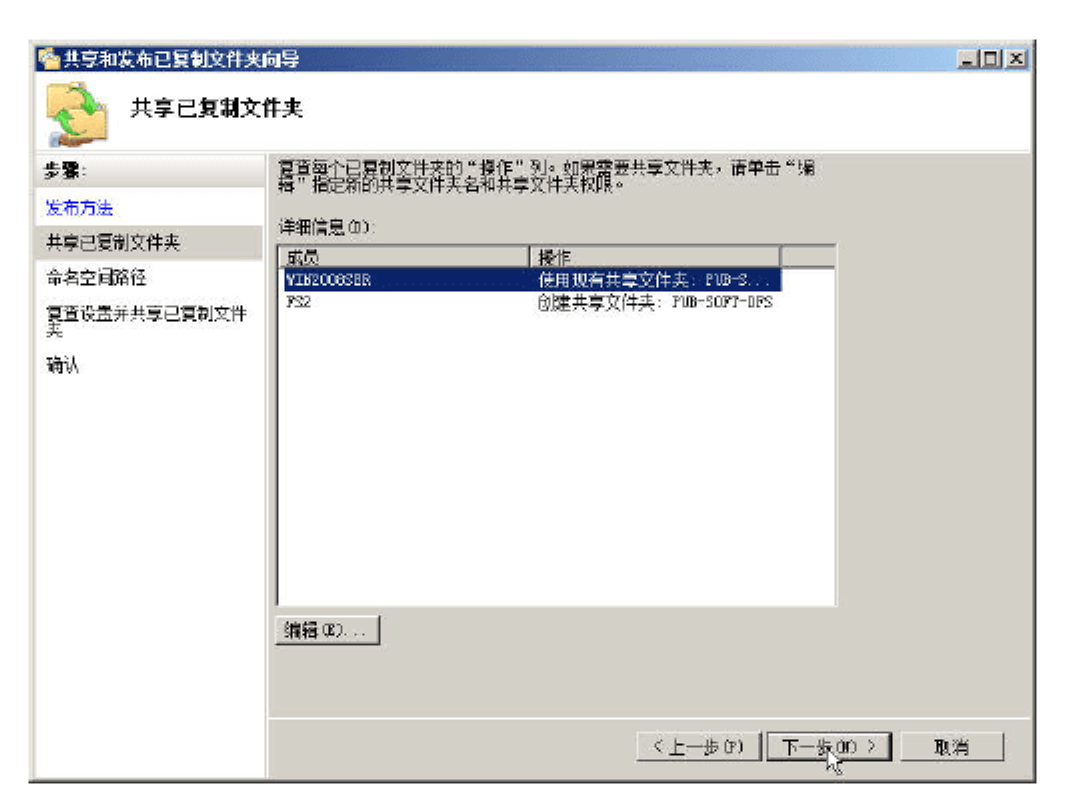


图 10-43　共享已复制文件夹



图 10-44　命名空间路径

05 在“复查设置并共享已复制文件夹”对话框，查看共享文件夹的设置，如图 10-45 所示。然后单击“共享”按钮，显示“确认”对话框，如图 10-46 所示。单击“关闭”按钮完成共享文件夹的发布。

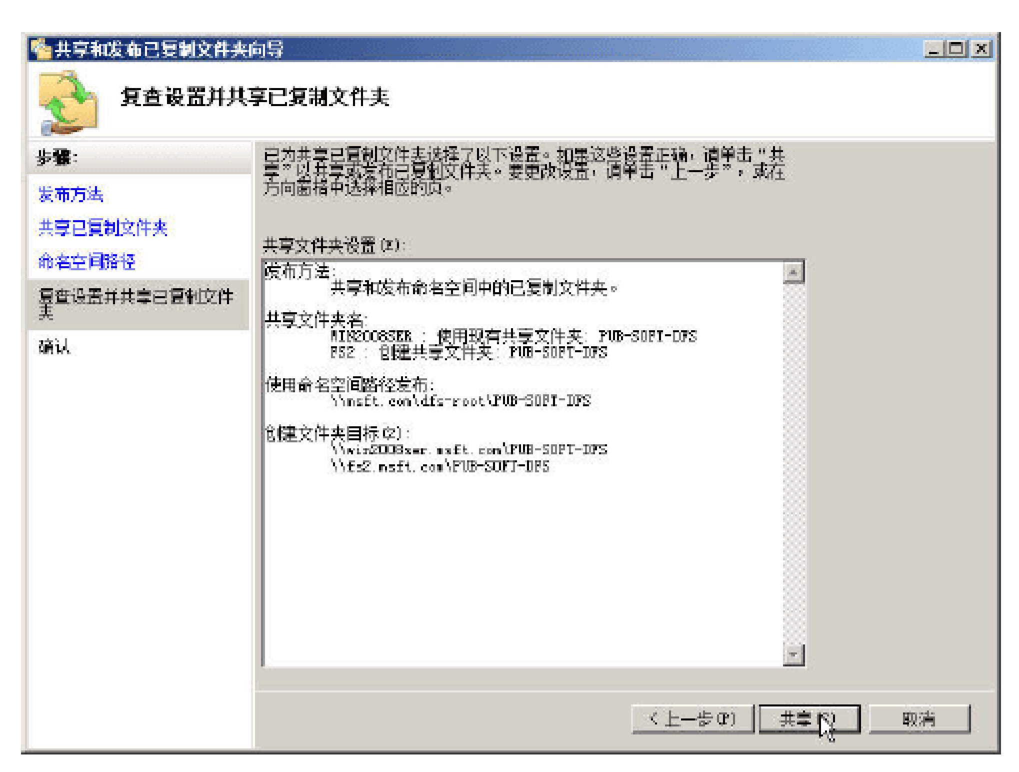


图 10-45　复查设置并共享已复制文件夹

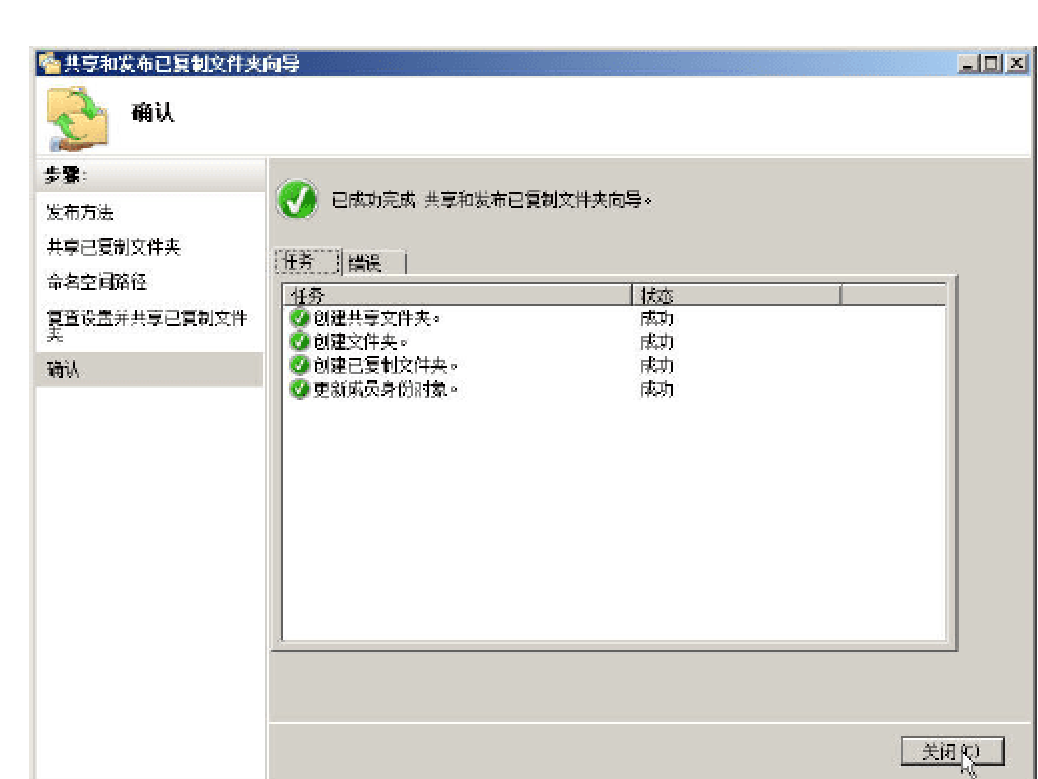


图 10-46　确认

10.3.5　DFS 复制计划管理

本节介绍 DFS 复制计划如何进行管理，具体步骤如下。

01 在“DFS 管理”窗口中，展开“复制”项，选择要修改的复制组，右击并从快捷菜单中选择“编辑复制组计划”命令，显示“编辑计划”对话框，如图 10-47 所示。

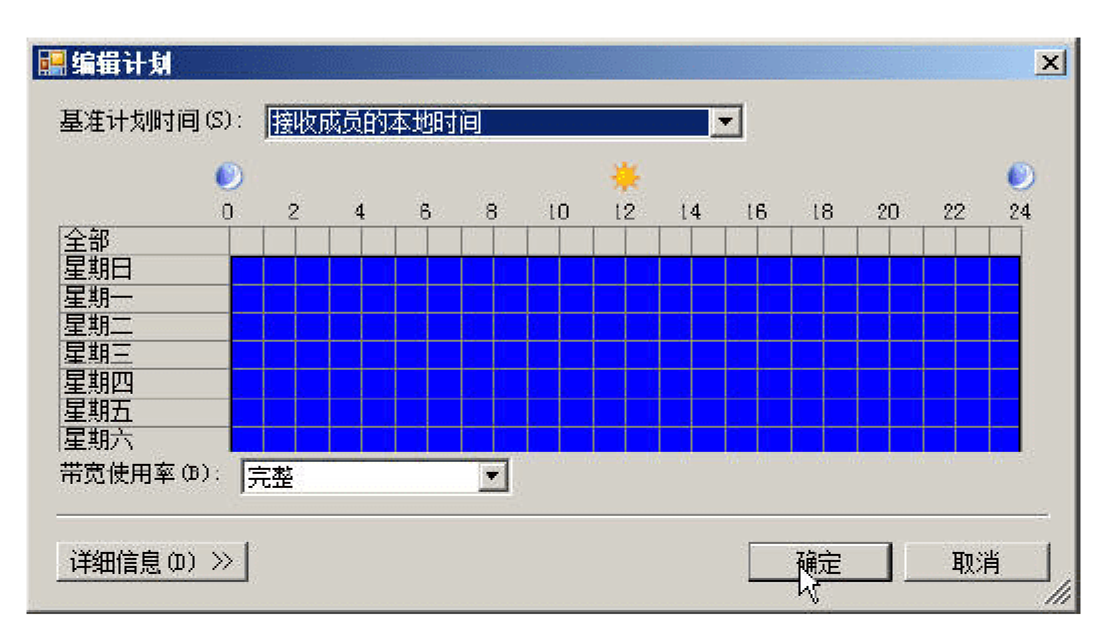


图 10-47　编辑计划

02 在图 10-47 中单击“详细信息”按钮，再单击“添加”按钮，将打开“添加计划”对话框，可根据需要设置计划时间，本例中设置为“8:00 ~ 22:00”，在“天”选项组中，把复选框全部选中，“带宽使用率”设置为“2Mbps”，如图 10-48 所示。

03 单击“确定”按钮返回，如图 10-49 所示，单击“确定”按钮完成复制组计划的设置。

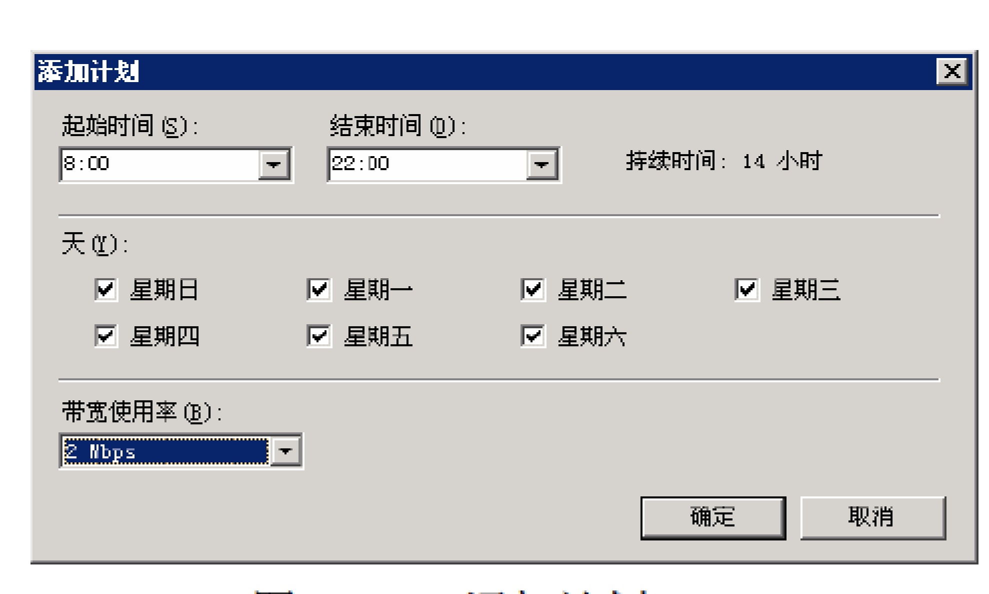


图 10-48　添加计划

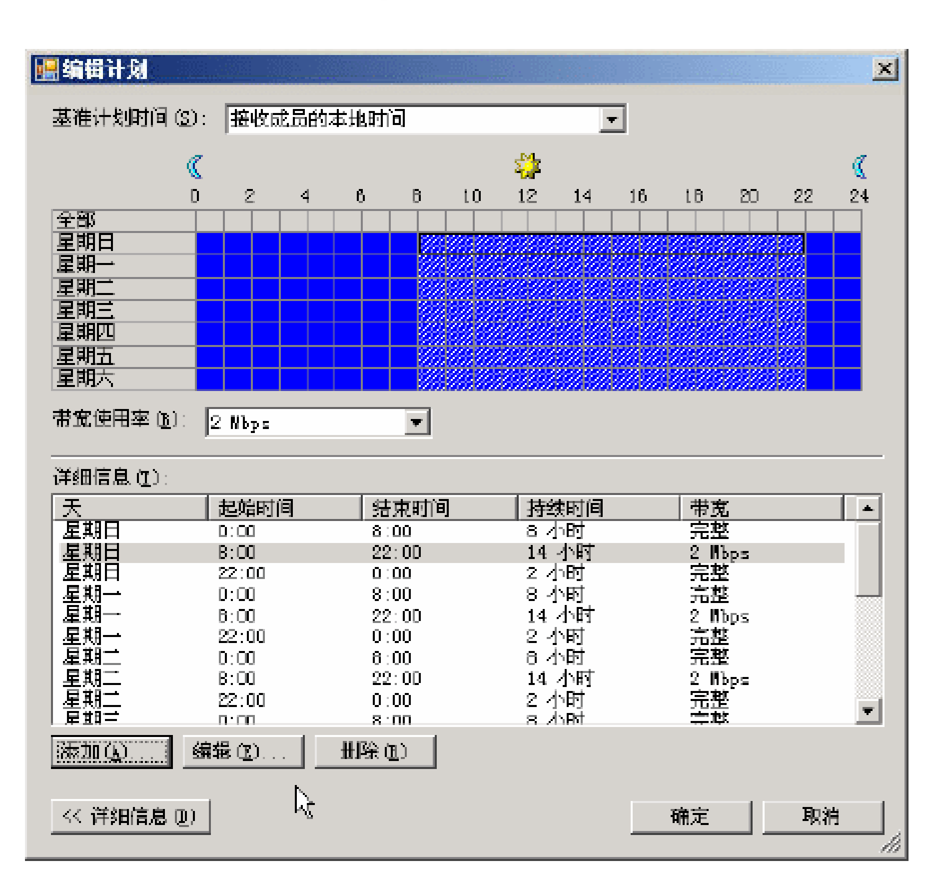


图 10-49　计划设置完成

DFS 复制创建并发布后，即可实现两台 DFS 服务器复制组的自动复制，这些不再一一介绍。

第 3 篇

Microsoft云计算应用平台与管理



第 11 章　Hyper-V Server 2008 R2 虚拟化产品配置、应用与管理

从本章开始，将介绍Microsoft最新的Hyper-V Server 2008 R2 SP1、Windows Server 2008 R2 SP1虚拟化技术，用 SCVMM 2008 R2 SP1 进行管理的相关内容，这些内容包括：

- 概述：是选择 Windows Server 2008 R2 还是 Hyper-V Server 2008 R2。
- 安装前注意事项，例如设置 BIOS、分区、磁盘选择等。
- 安装 Windows Server 2008 R2 并添加 Hyper-V 功能。
- Hyper-V 安装与配置。
- 理解 Hyper-V 虚拟网络。
- Hyper-V 基本操作，创建虚拟机，管理虚拟机，导入、导出虚拟机，使用差异磁盘创建虚拟机。
- SCVMM 安装配置、规划。
- SCVMM 基本操作。
- SCVMM 企业应用：管理多台 Hyper-V、迁移、群集等。

本章先介绍 Hyper-V Server 2008 R2 的使用，在下一章将介绍 SCVMM 2008 R2 的内容。

11.1　为虚拟化主机选择合适的版本

Hyper-V Server 2008 R2 与 Windows Server 2008 R2 都提供了虚拟化功能，对于用户来说，应该怎样选择呢？

Windows Server 2008 R2 是 Microsoft 最新的服务器操作系统，只有 64 位版本，这个产品集成了 Hyper-V 的功能。如果需要虚拟化的主机数量比较少，并且需要在虚拟化主机上直接管理，同时还需要其他的网络服务，例如 DHCP、DNS、IIS 等，则可以选择 Windows Server 2008 R2 并添加 Hyper-V 功能。但是，这个产品是一个商业软件，需要付费。

Hyper-V Server 2008 R2，可以看作 Windows Server 2008 R2 的 Core 版本并添加了 Hyper-V 功能，这个产品需要专门的管理计算机。例如，可以使用网络中的 Windows 7、Windows Server 2008 或 SCVMM 2008 R2 进行管理。由于减少了图形界面以及其他不需要的网络服务功能，相比

Windows Server 2008 R2，Hyper-V 会更加高效。

Hyper 是一款免费产品，所有用户都可以从 Microsoft 官方网站下载并免费使用。如果用户只需要虚拟化主机，并且物理主机不对外提供其他服务，可以选择这个产品。

如果使用 Windows Server 2008 或 Windows 7 管理 Hyper-V Server 2008 R2，与使用 Windows Server 2008 R2 并安装 Hyper-V 功能，相差并不大，但为了远程管理 Hyper-V，还需要在 Hyper-V 的主机上做一些配置。在本章中，我们准备了两台服务器，其中一台安装 Windows Server 2008 R2，另一台安装 Hyper-V Server 2008 R2（都升级到 SP1 补丁），下文对此进行详细介绍。

11.2　系统需求

Windows Server 2008 R2（启用 Hyper-V 技术）与 Hyper-V Server 2008 R2 的硬件需求如下：

- 处理器技术：64 位 Intel VT 或 AMD-V、硬件 DEP、Intel XD bit 或 AMD Nx bit。
- 处理器频率：最低 1.4GHz，推荐 2.0GHz 或更高。
- 内存容量：最少 1GB，推荐 2GB 或更多。
- 硬盘空间：最少 8GB，推荐 20GB 或更多。

Hyper-V Server 2008 R2 支持的虚拟操作系统（括号内为可分配物理处理器数量）：

- Windows Server 2008 R2（1/2/4）。
- Windows Server 2008 x64/x86（1/2/4）。
- Windows Server 2003 R2 x64/x86（1/2）。
- Windows Server 2003 x64/x86（1/2）。
- Windows Server 2000（1）。
- SUSE Linux Enterprise Server 11 x64/x86（1）。
- SUSE Linux Enterprise Server 10 SP2 x64/x86（1）。
- Red Hat Enterprise Linux 5.2/5.3 x64/x86（1）。
- Windows 7 x64/x86（1/2/4）。
- Windows Vista x64/x86（1/2）。
- Windows XP x64/x86。

11.3　安装前的注意事项

在安装 Windows Server 2008 R2（或 Hyper-V Server 2008 R2，以后统一用 Hyper-V Server 2008 代替）时，需要注意以下问题。

（1）检查计算机是否符合安装的最低要求。一般情况下，内存与硬盘空间都会满足要求，需要注意的是 CPU 及其相关设置。如果是在 IBM、DELL、HP 等服务器上安装则，则最近几年购买

的服务器都支持 Hyper-V 技术；如果是浪潮服务器，须检查 CMOS 中是否可以启用 Intel VT 与 DEP，如果没有相关选项，须联系厂家，以获得 BIOS 的更新程序。

在安装之前，须先进入 CMOS 设置选项（不同厂家的服务器，进入 CMOS 设置的按键不同，须注意屏幕提示。目前，对于大多数服务器来说，是按 F2 键），在“Advanced Processor Options”处按回车键，进入高级处理器设置页，启用 Intel VT 技术（如图 11-1 所示）。

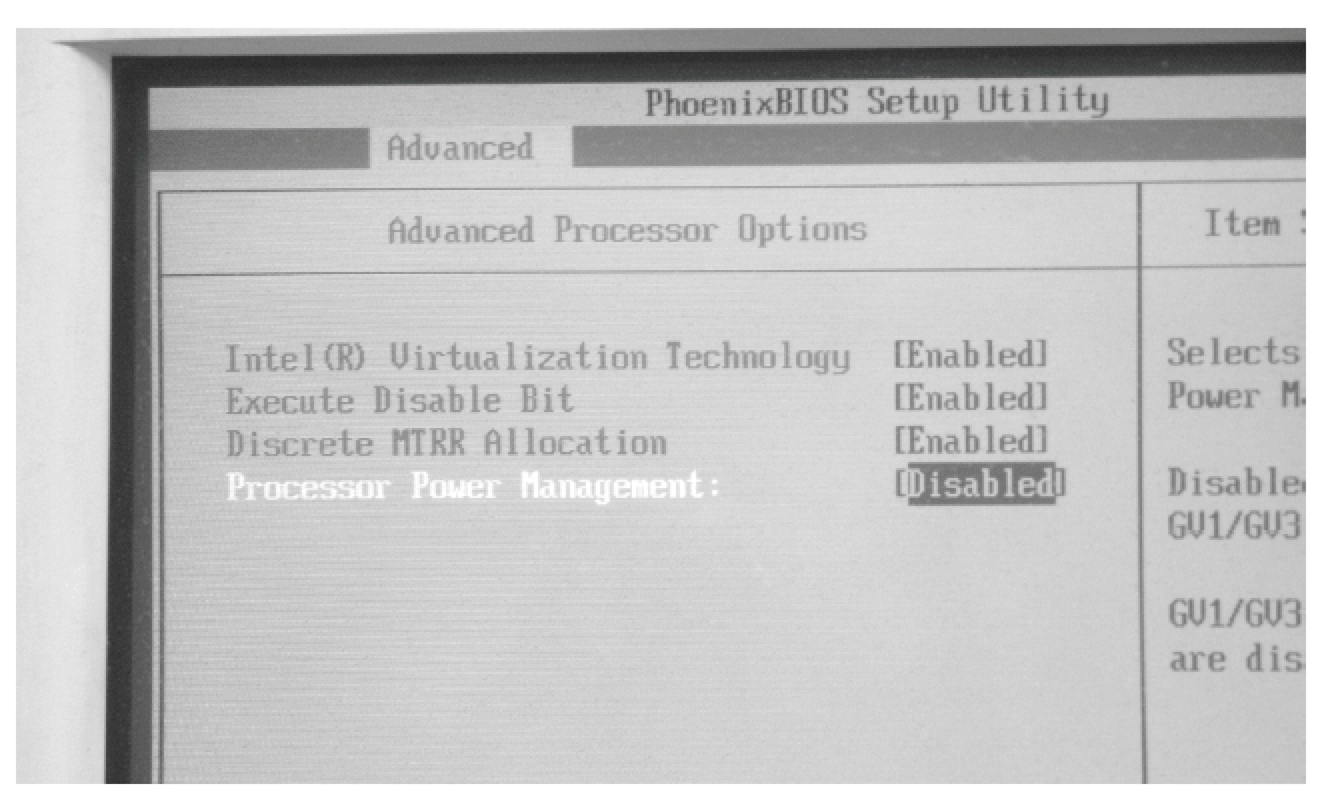


图 11-1

（2）在安装之前，要规划好服务器的硬盘。建议在服务器上配置至少 3 块硬盘做 RAID5，如果有 6 块及以上的偶数硬盘，建议用 RAID50，这样可以在性能、安全性上有个折衷。另外，在配置 RAID5 或 RAID50 的时候，建议划分为 2 个逻辑磁盘，其中第 1 个逻辑磁盘在 100GB 左右，这个用来安装操作系统，剩下的按照每个 2TB 的大小，划分成多个逻辑磁盘。例如，一台 HP DL380G7，配置了 6 个 500GB 的硬盘，采用 RAID50，划分第 1 个逻辑磁盘为 100GB，第 2 个逻辑磁盘为 2TB，第 3 个逻辑磁盘为 500GB×6–100GB–2TB≈900GB。

11.4 实验环境

为了全面介绍 Windows Server 2008 R2 与 Hyper-V Server 2008 R2，我们准备了 6 台服务器，各服务器相关参数如表 11-1 所示。

表 11-1 各服务器相关参数

服务器厂商	计算机名称	IP 地址	作用
DELL	DC.heinfo.local	172.30.5.15	heinfo.local 的第一台域控制器
DELL	wsus	172.30.5.6	WSUS 服务器，为其他计算机提供补丁服务
DELL	WSS2008R2	172.30.5.5	Windows Storage Server 2008 R2，为虚拟机以及其他服务器提供网络存储服务
联想	datacenter	172.30.5.16	heinfo.local 的第二台域控制器
浪潮	ws08r2-hyper-v	172.30.5.31	Windows Server 2008 R2，添加 Hyper-V 功能，本次实验的“主力”
浪潮	Hyper-V-2008R2	172.30.5.17	Hyper-V Server 2008 R2，另一台虚拟化主机

各服务器用千兆网络连接，摆列图如图 11-2 所示。网络拓扑如图 11-3 所示。



图 11-2　服务器外形图

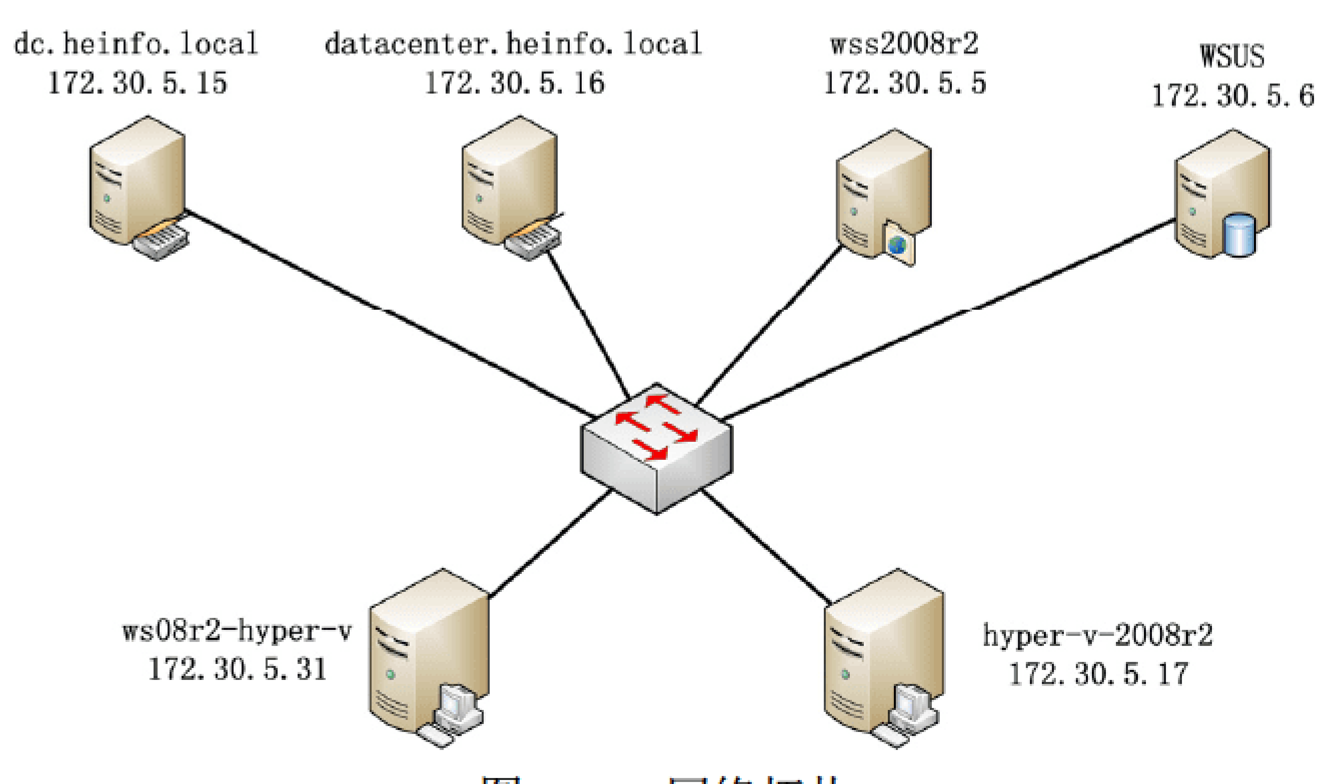


图 11-3　网络拓扑

在图 11-3 的网络拓扑中，172.30.5.15、172.30.5.16 的 Active Directory 服务器，172.30.5.5 的 Windows Storage Server 2008 R2 存储服务器以及 172.30.5.6 的 WSUS 服务器，已经提前安装配置好。如果需要了解这方面的内容，可参考本书第 6 章的相关内容。本章只介绍 172.30.5.31 与 172.30.5.17 这两台服务器的安装与配置。

11.5　安装 Windows Server 2008 R2 并添加 Hyper-V 功能

在第 1 台浪潮服务器上，规划服务器的硬盘，然后安装 Windows Server 2008 R2 Datacenter，安装完成之后，添加 Hyper-V 功能，主要步骤如下。

01 使用 Windows Server 2008 R2 的安装光盘，启动安装，在“选择要安装的操作系统”对话框中，选择“Windows Server 2008 R2 Datacenter（完全安装）”选项，如图 11-4 所示。也可以选择企业版，不推荐选择标准版与 Web 服务器版本。

02 单击“下一步”按钮，在“您想进行何种类型的安装”对话框中，选择“自定义（高级）”选项。

03 在“您想将 Windows 安装在何处”对话框中，选择第 1 个分区，在本例中，这是用 RAID

卡划分的第 1 个逻辑磁盘，如图 11-5 所示。

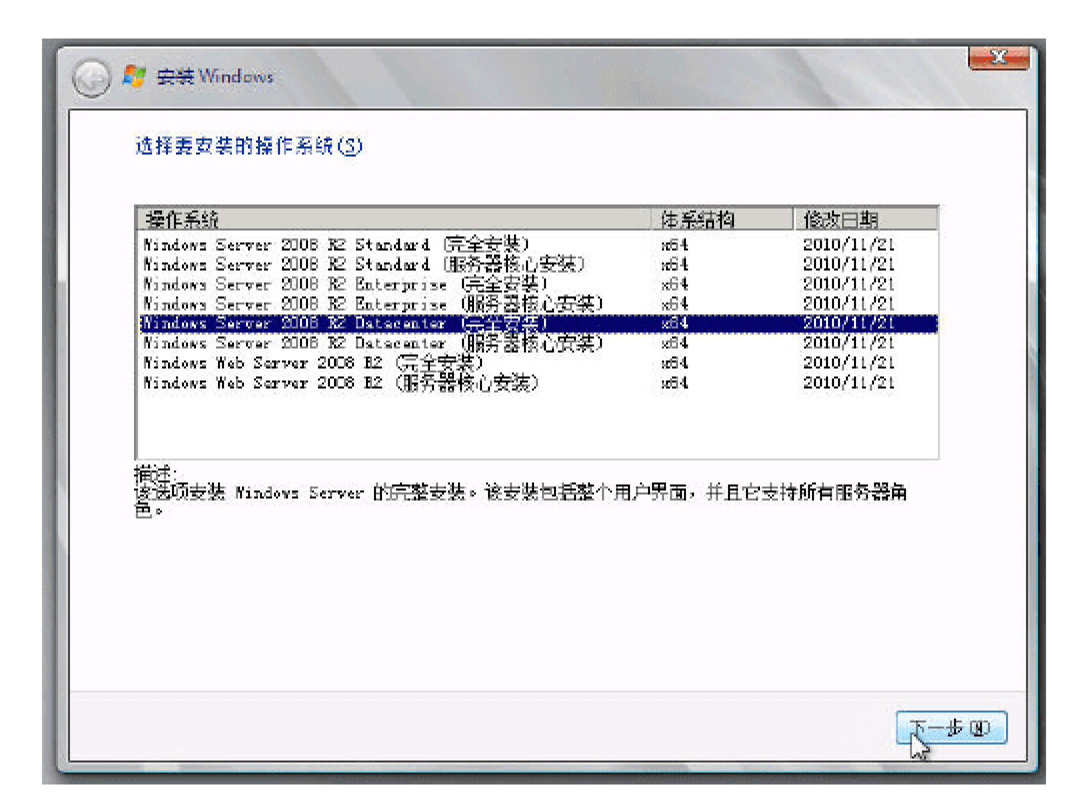


图 11-4 选择要安装的版本

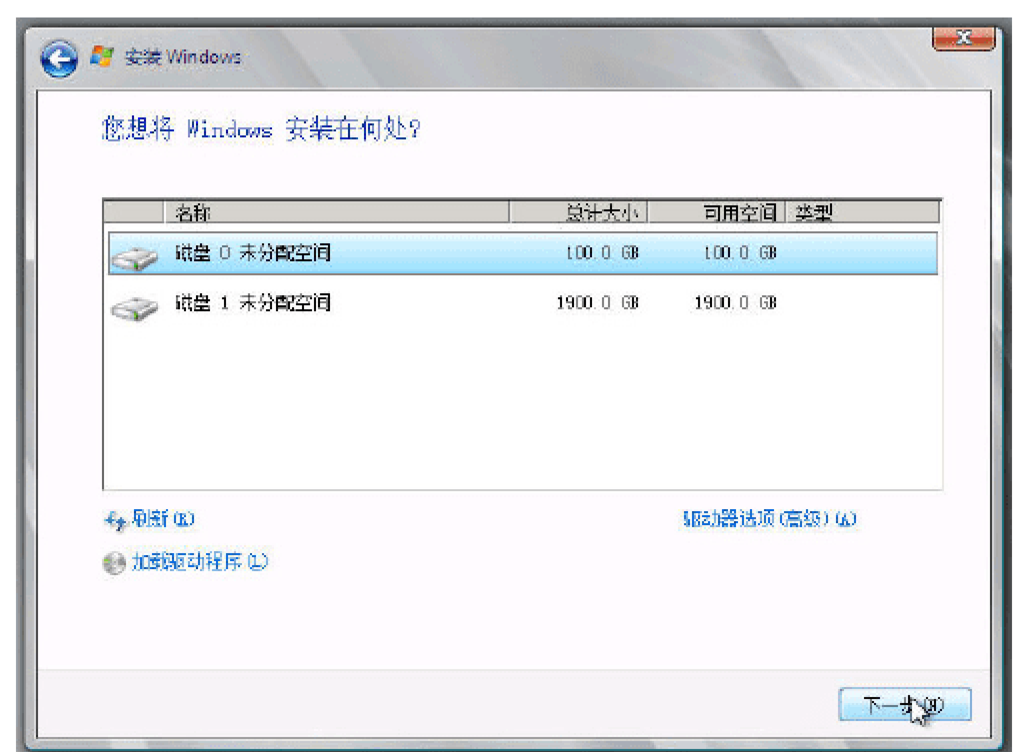


图 11-5 选择磁盘

04 安装完成后，在第 1 次登录之前更改密码。

05 进入系统后，修改计算机名称，然后重新启动计算机，如图 11-6 所示。

06 再次进入系统后，设置 IP 地址为 172.30.5.31，设置 DNS 为 172.30.5.15 或 172.30.5.16，然后将计算机加入到 heinfo.local 域，如图 11-7 所示。加入到域完成后，重新启动计算机。



图 11-6 修改计算机名称

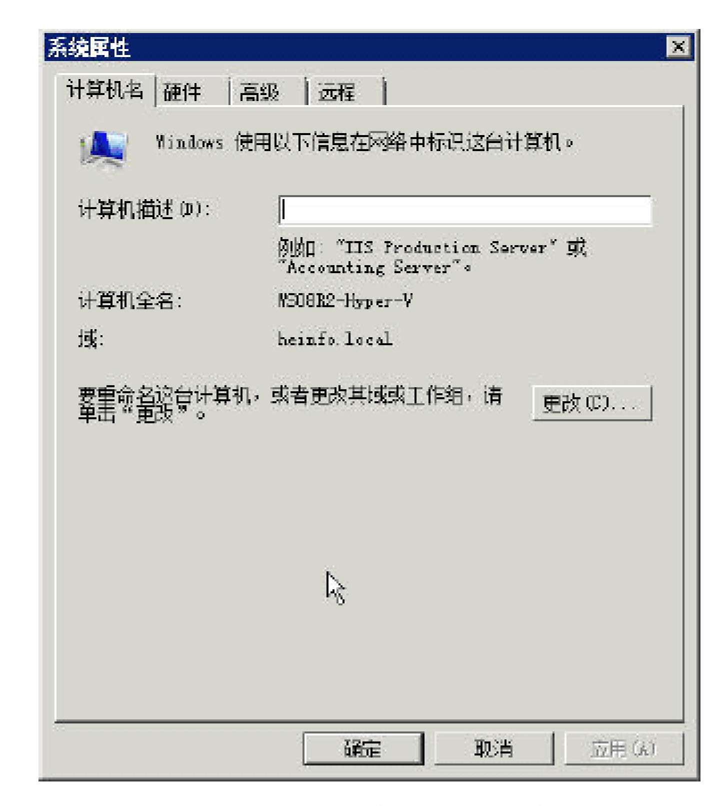


图 11-7 加入到域

07 第 3 次进入系统后，进入“服务器管理器”，添加 Hyper-V 功能，如图 11-8 所示。



图 11-8 添加 Hyper-V

08 在安装的过程中，选择一块网卡，作为虚拟网络与其他计算机进行通信，如图 11-9 所示。有关虚拟网卡我们将在后文介绍。

09 安装完成之后，根据提示重新启动计算机，如图 11-10 所示。



图 11-9 选择网卡



图 11-10 重新启动

至此，第 1 台虚拟化主机安装完成。

11.6 安装 Hyper-V Server 2008 R2 并配置远程管理

本章介绍，在第 2 台浪潮服务器上，安装 Hyper-V Server 2008 R2。同样，还是采用光盘安装（如果 Microsoft 修改远程安装错误，则可以通过“Windows 部署服务”远程安装，笔者的 Windows Server 2008、Hyper-V Server 2008 都曾经远程部署过）。与 Windows Server 2008 R2 不同，在安装完 Hyper-V Server 2008 R2 之后，还需要启用一些配置才能进行管理。下面分别介绍 Hyper-V Server 2008 R2 的安装与配置。

11.6.1 Hyper-V Server 2008 R2 安装与更新

在本文完稿前，Microsoft 还没有推出集成 SP1 的 Hyper-V Server 2008 R2。用户可以安装 Hyper-V Server 2008 R2，安装完成之后，再安装 Windows Server 2008 SP1 补丁进行升级。本次实验中，我们将通过网络中的 WSUS 服务器完成所有的补丁的升级。

01 使用 Hyper-V Server 2008 R2 安装光盘启动服务器，在安装语言界面选择“我的语言为中文（简体）”选项，如图 11-11 所示。

02 在“您想将 Windows 安装在何处”界面中，创建一个 100GB 左右的分区用来安装 Hyper-V Server 2008 R2，如图 11-12 所示。在本例中，我们的服务器安装了一个 1TB 的 SATA 硬盘（你没有看错，正在使用的服务器除了支持 SAS 硬盘，还支持 SATA 硬盘），在创建 100GB 左右的分区时，Hyper-V Server 2008 R2 安装程序会自动划分一个 100MB 的分区用于系统保留。

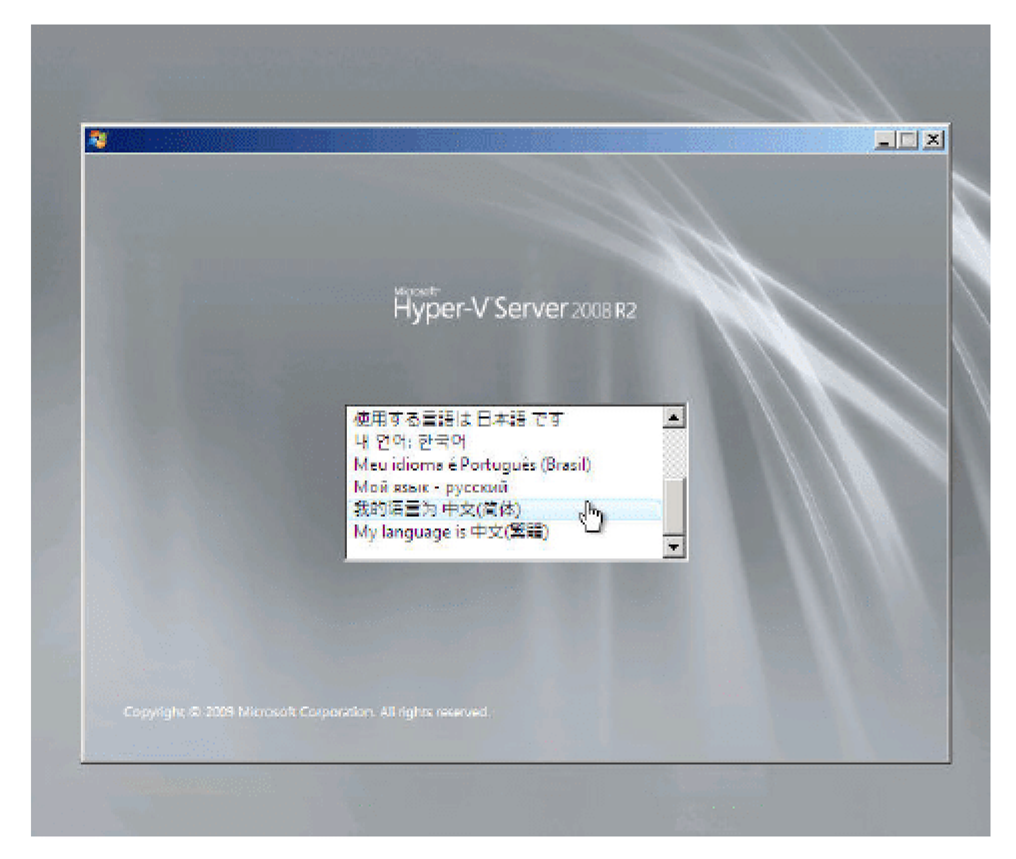


图 11-11 选择安装语言

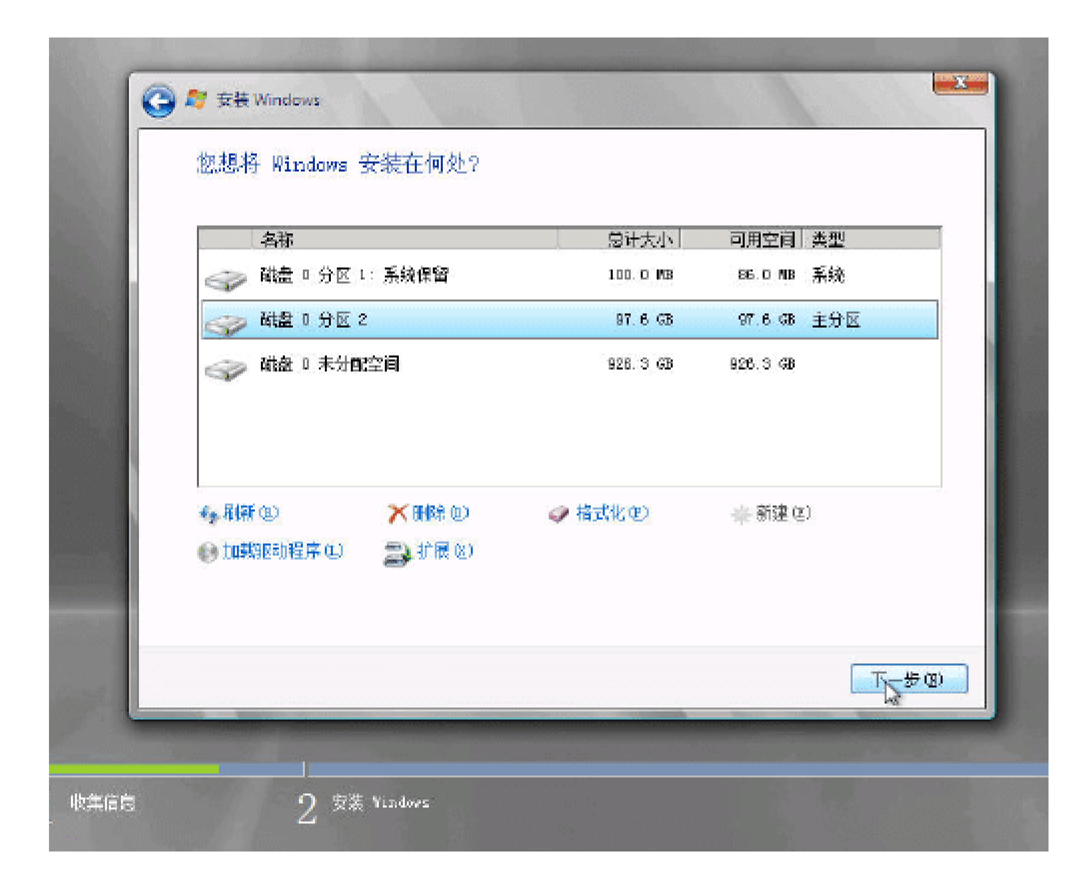


图 11-12 选择安装磁盘并创建分区

03 在安装完成之后，进入 Hyper-V Server 2008 R2，如图 11-13 所示。Hyper-V Server 2008 R2 只有一个文本管理界面，如图 11-13 所示。



图 11-13 Hyper-V 管理界面

11.6.2 将 Hyper-V Server 2008 R2 加入到域并安装最新补丁

进入 Hyper-V Server 2008 R2 管理界面之后，修改计算机的名称，重新启动，加入到域、下载并安装最新的补丁，主要步骤如下。

01 在 Hyper-V 管理界面中，在“输入数字来选择选项”后面输入想要执行的命令，首先输入 2，然后按回车键，为 Hyper-V Server 2008 R2 计算机设置新的名称。在本例中，这个名称为“Hyper-v-2008r2”，设置完成之后，根据向导提示重新启动计算机。

02 再次进入计算机后，在“输入数字来选择选项”后输入数字 8，设置当前计算机的 IP 地址为 172.30.5.17，设置 DNS 为 172.30.5.15、172.30.5.16。设置 IP 地址之后，输入数字 1 并按回车键，将计算机加入到域，在本例中，域名为 heinfo.local，如图 11-14 所示。加入到域之后，重新启动计算机。

03 第 3 次进入系统后，在“输入数字来选择选项”后输入数字 6，下载并安装更新。如图 11-15 所示。




图 11-14　将计算机加入到域

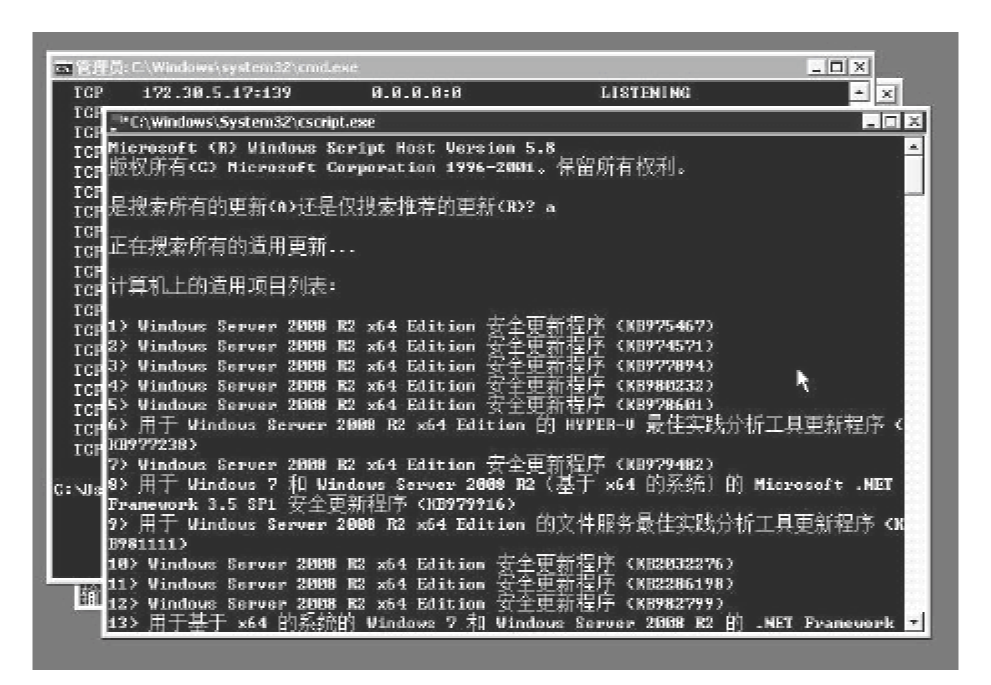
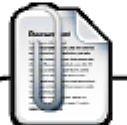


图 11-15　检查并安装更新



说 明

在本次实验中，是使用网络中的 WSUS 服务器进行 Hyper-V Server 2008 的补丁安装。并且，是在 172.30.5.15 或 172.30.5.16 的“域控制器”中，通过修改组策略，为域中的所有计算机配置为采用 WSUS 服务器进行更新。

04 安装完更新之后，重新启动计算机。如果更新比较多，有的时候一次不能下载并安装完所有的更新。第 4 次进入系统后，须再次检查并安装更新，直到所有的更新都全部安装完成为止。图 11-16 是将 Hyper-V Server 2008 R2 升级到 SP1 之后的截图。

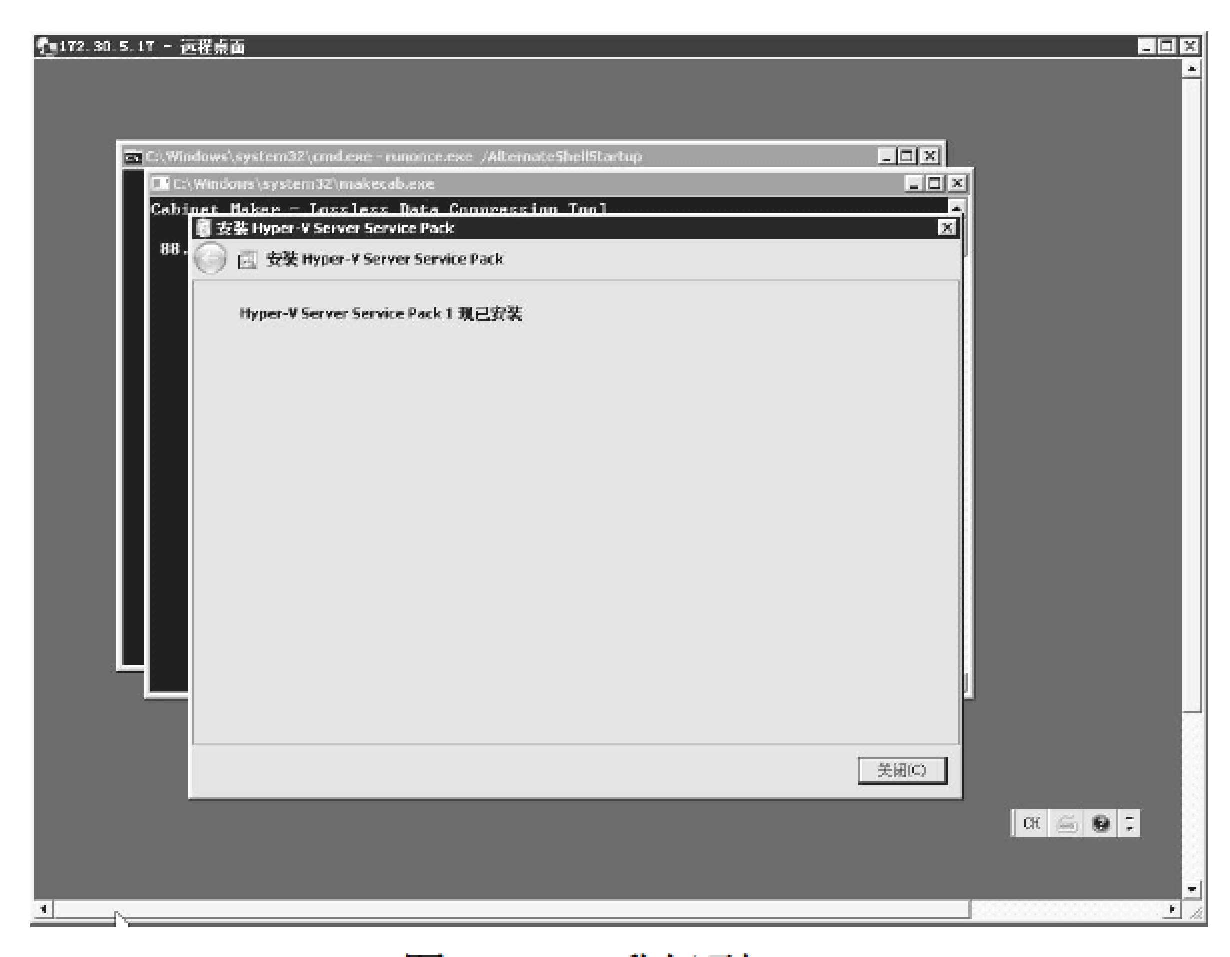


图 11-16　升级到 SP1

11.6.3　配置 Hyper-V Server 2008 R2 用于远程管理

在将 Hyper-V 加入到域并安装最新的补丁后，配置 Hyper-V 并允许远程管理，步骤如下。

01 在 Hyper-V Server 2008 R2 管理界面选择“配置远程管理”，并依次配置“允许 MMC 远程管理”、“启用 Windows PowerShell”、“允许服务器管理器远程管理”，如图 11-17 所示。在配置远程管理的过程中，根据屏幕提示，重新启动计算机。

02 在网络中的另外一台计算机上，在 IE 浏览器中打开 http://archive.msdn.microsoft.com/HVRemote 页，下载 Hyper-V Remote Management Configuration Utility 程序，这是一个名为

HVRemote.wsf、大小为 249KB 的程序。下载之后，通过共享文件夹复制到 Hyper-V 计算机的 C 盘或 D 盘，然后再次返回到 Hyper-V Server 2008 R2，在命令提示窗口中执行如下的命令：

```
cscript hvremote.wsf /mode:server   /add:heinfo\administrator
```

这条命令是为 Hyper-V Server 2008 R2 添加一个用于远程管理的账户，本例中这个账户是 heinfo 域的 Administrator。执行界面如图 11-18 所示。



图 11-17　配置远程管理



图 11-18　在服务器上添加远程管理账户

在以后的工作中，我们将使用 IP 地址为 172.30.5.31 的 Windows Server 2008 R2 管理 Hyper-V Server 2008 R2，或者使用 SCVMM 2008 R2 管理 Hyper-V Server 与 Windows Server 2008 R2。接下来还要为远程管理 Hyper-V Server 2008 R2 做进一步的配置，步骤如下。

01 在 Windows Server 2008 R2 计算机上，运行下载的 HVRemote.wsf，命令格式如下：

```
cscript   hvremote.wsf   /mode:client   /mmc:enable
```

命令执行过程如图 11-19 所示。

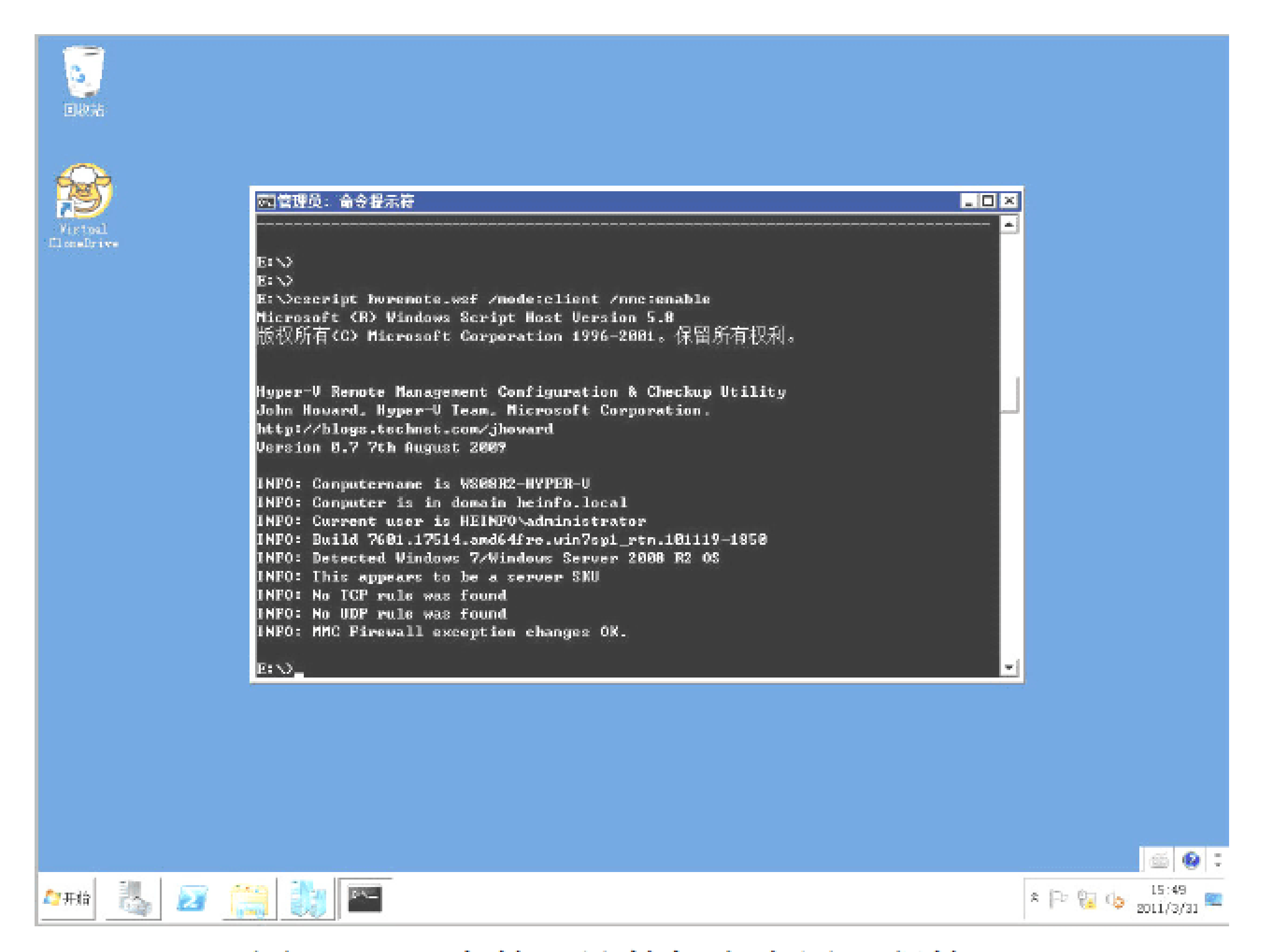


图 11-19　在管理计算机上启用远程管理

02 运行 MMC，添加“高级安全 Windows 防火墙→选择另一台计算机→输入 Hyper-V Server 2008 R2 的 IP 地址（本例为 172.30.5.17）”，然后在“入站规则”中启用“Windows Management Instrumentation”相关的 3 条规则，如图 11-20 所示。

然后在“出站规则”中，启用“Windows Management Instrumentation（WMI-Out）”规则，如图 11-21 所示。

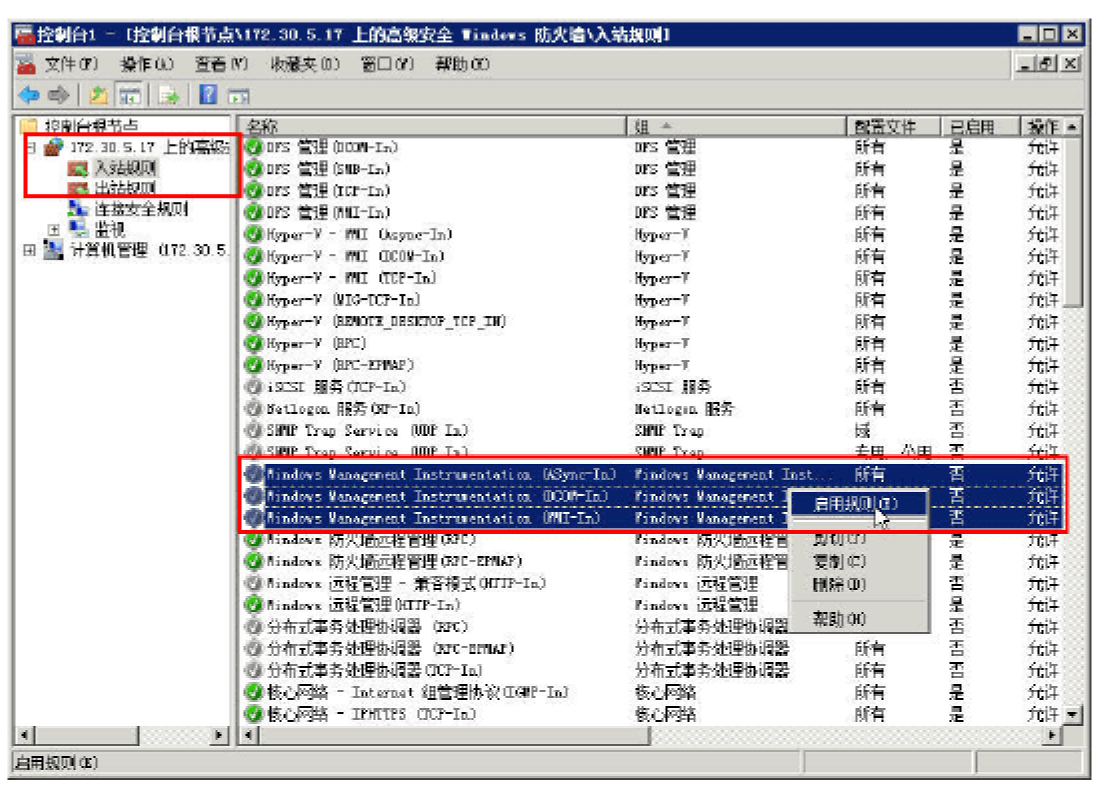


图 11-20　启用入站规则

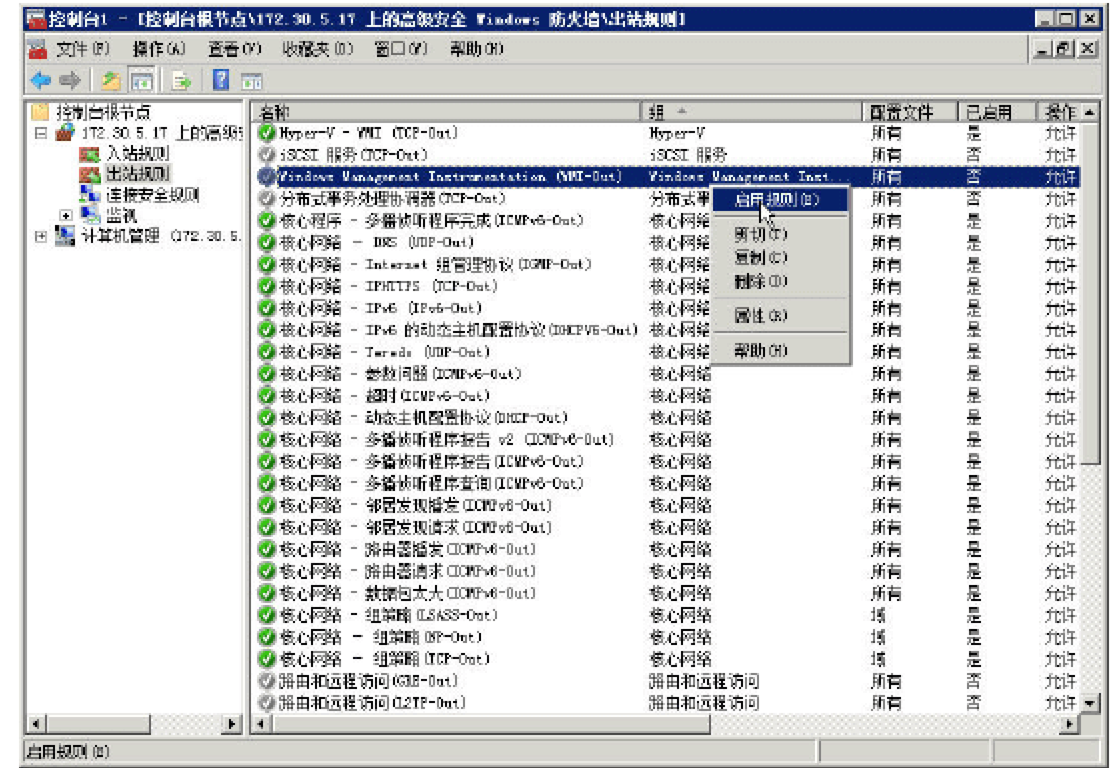


图 11-21　启用出站规则

经过上述配置，就可以管理 Hyper-V Server 2008 R2 了，步骤如下。

01 以域管理员的身份登录到 Windows Server 2008 R2，在用户名处输入 heinfo\administrator，然后输入管理员密码，如图 11-22 所示。

02 从“管理工具”中打开 “Hyper-V 管理器”选项，右击“Hyper-V 管理器”，在弹出的快捷菜单中选择“连接到服务器”选项，如图 11-23 所示。



图 11-22　以域管理员身份登录

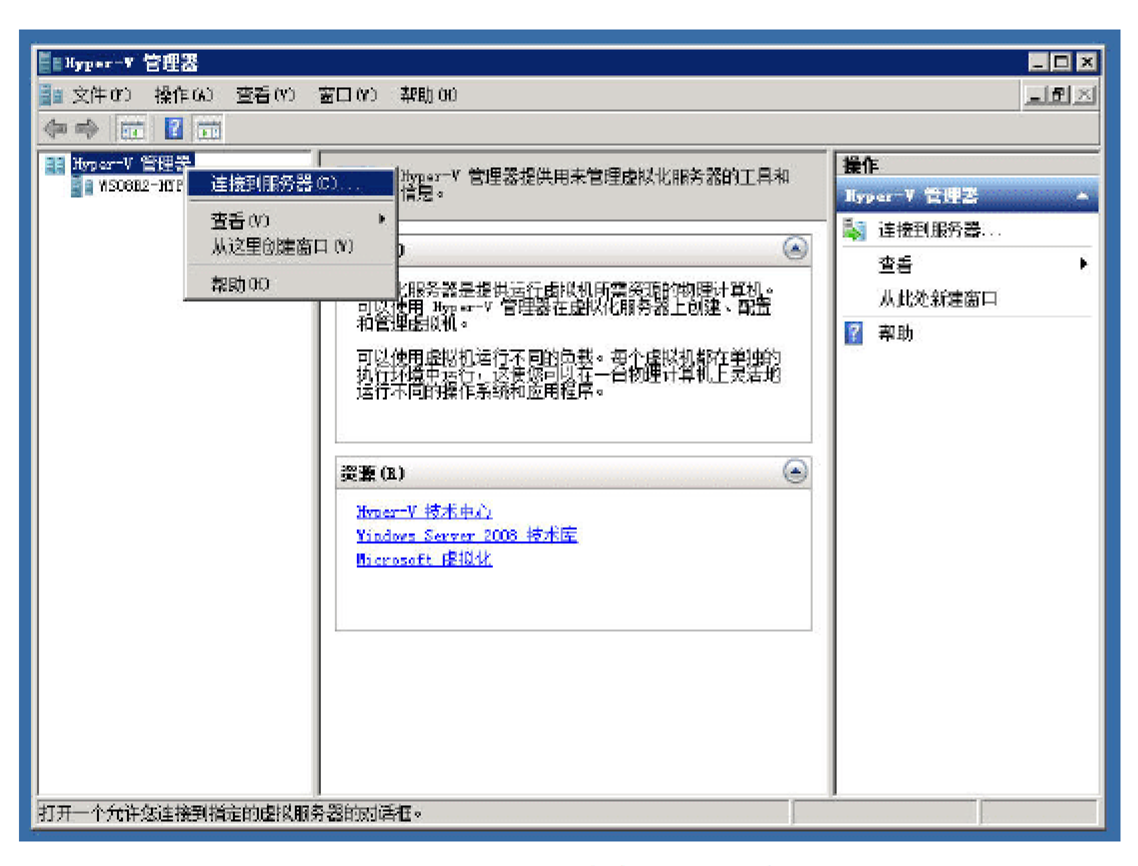


图 11-23　连接到服务器

03 在“选择计算机”对话框中，选择“另一台计算机”单选按钮，并输入要管理的 Hyper-V Server 2008 R2 计算机的 IP 地址或计算机名称，然后单击“确定”按钮，如图 11-24 所示。

04 略等一下，就可以连接到 Hyper-V Server 2008 R2，如图 11-25 所示。由于 Hyper-V Server 2008 R2 还没有创建虚拟机，所以在“虚拟机”列表中没有显示。

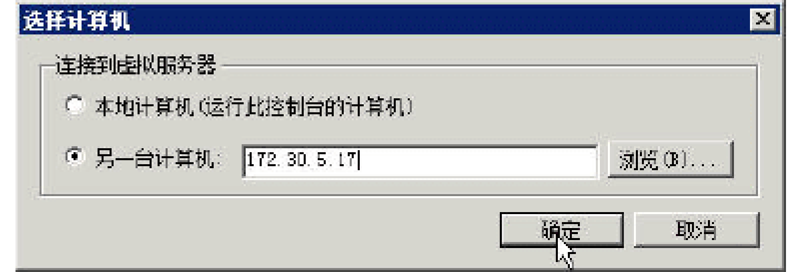


图 11-24　连接到另一台计算机

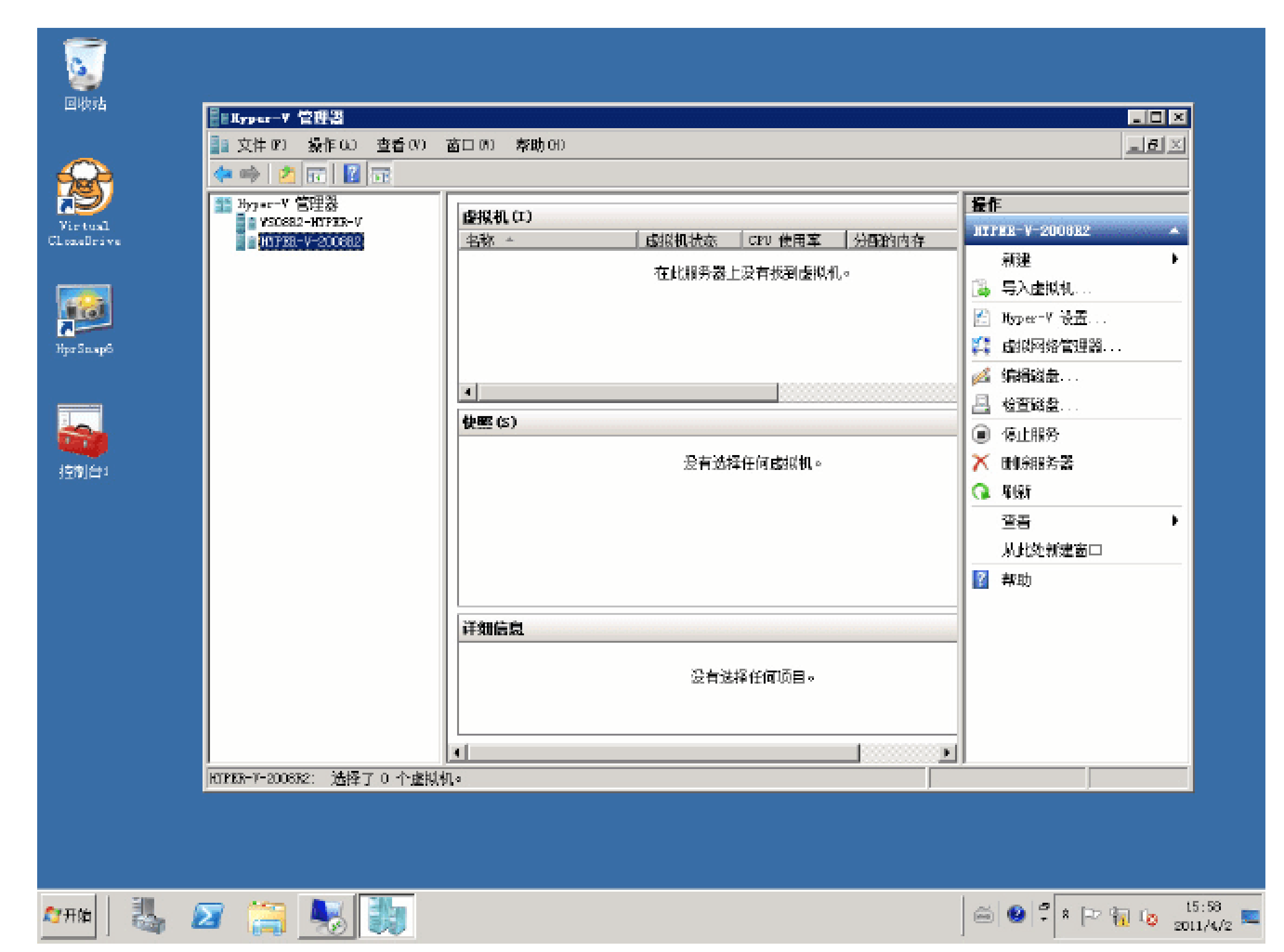


图 11-25　连接到 Hyper-V Server 2008 R2

在使用“Hyper-V 管理器”连接到 Hyper-V Server 2008 R2 之后，管理 Hyper-V Server 2008 R2，与使用 Windows Server 2008 R2 启用 Hyper-V 功能之后，创建、管理与使用虚拟机，以及管理虚拟网络之后的步骤，都是相同的。在以后的管理中，我们将不再对这两台服务器加以区别。

05 使用远程桌面连接到 Hyper-V Server 2008 R2，进入命令提示符，格式化 D 盘，然后创建一个文件夹用来保存虚拟机。在本例中，创建的文件夹名为“Hyper-V”，如图 11-26 所示。

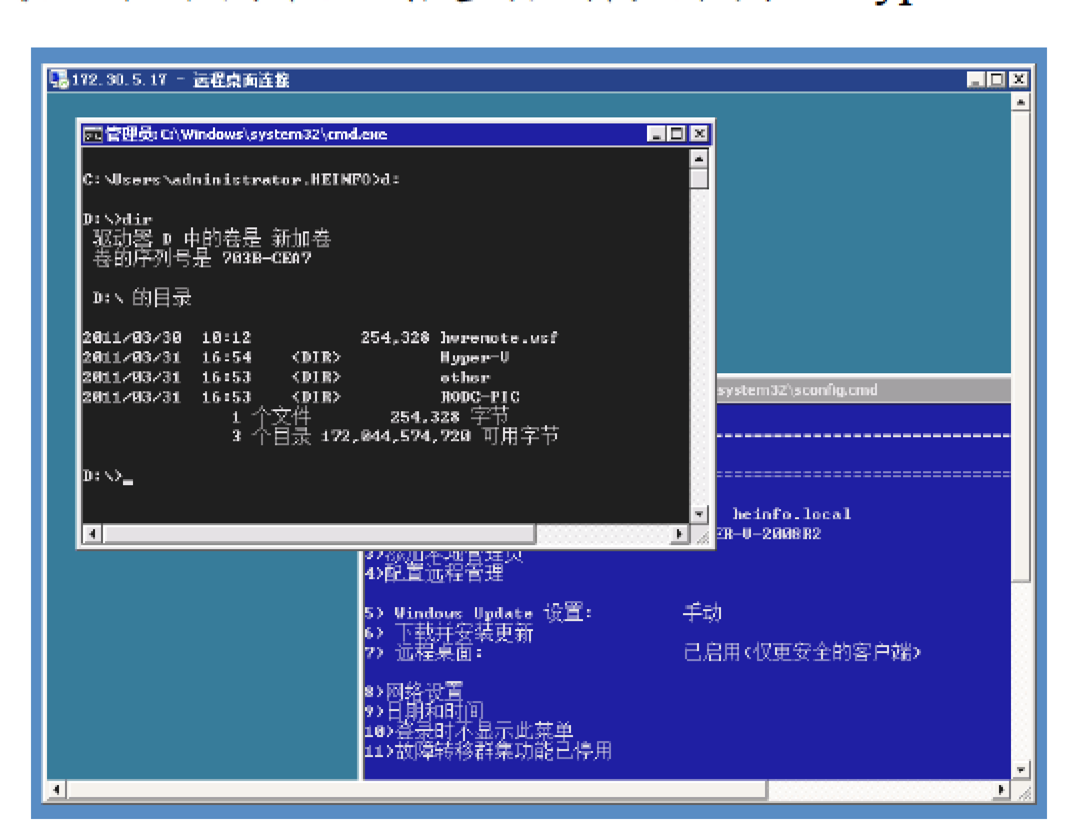


图 11-26　创建文件夹用来保存虚拟机

11.7　理解并配置 Hyper-V 虚拟网络

在 Hyper-V 中，虚拟网络分为 3 种：“外部”、“内部”、“专用”。这些虚拟网络与主机、虚拟机以及网络中其他计算机的关系，如图 11-27 所示。

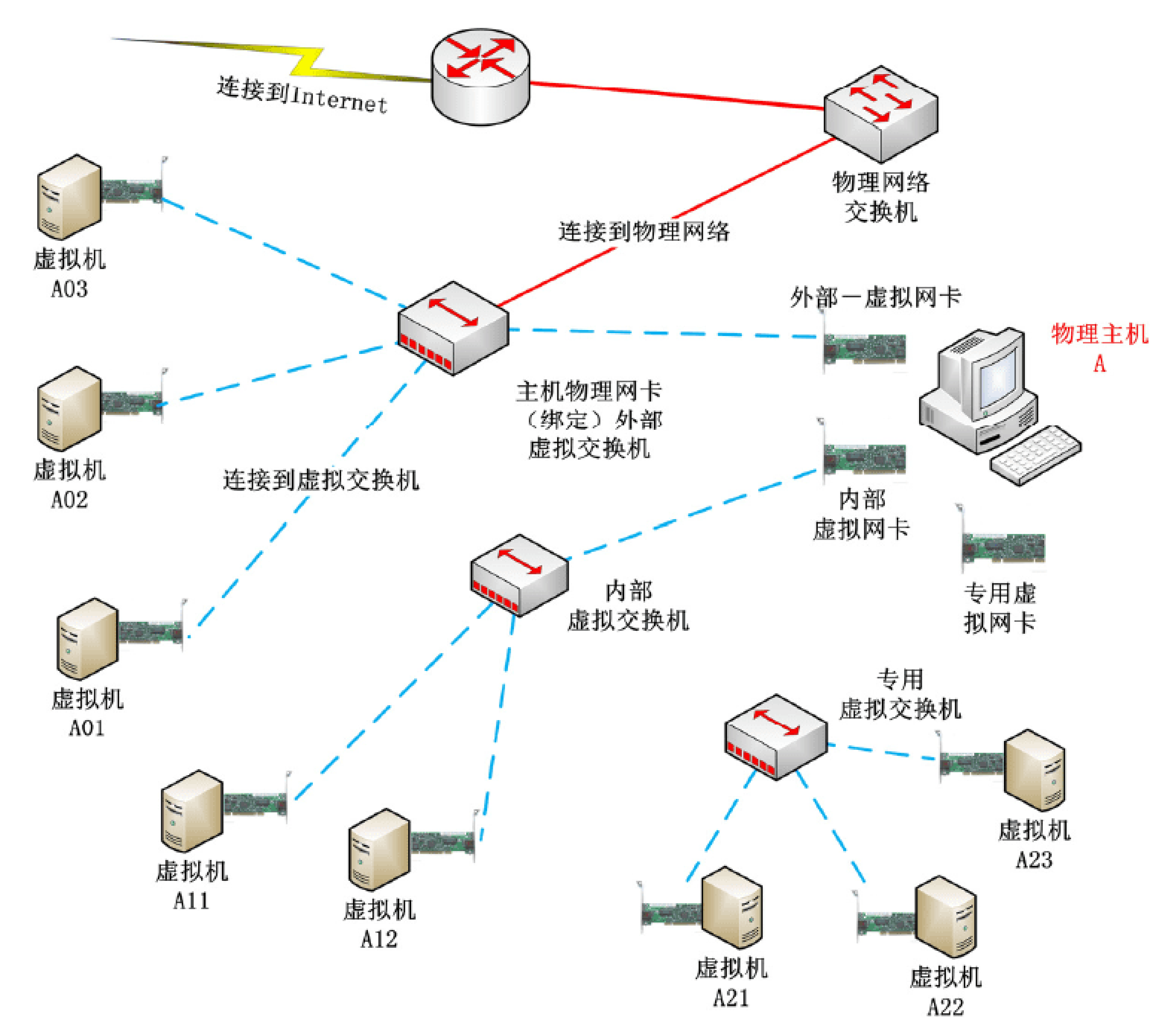


图 11-27　Hyper-V 虚拟网络

“外部”虚拟网络，是 Hyper-V 通过将“Microsoft 虚拟交换机协议”绑定在主机网卡上实现的。如果虚拟机选择“外部”虚拟网络，则虚拟机“相当”于网络中的一台计算机，是可以与物理网络中的其他计算机、主机互相访问的。例如，在图 11-27 中，虚拟机 A01、A02、A03 与物理主机 A 以及同一网络的其他计算机是可以互相访问的。虚拟机 A01、A02、A03 也能访问 Internet。

“内部”虚拟网络只允许虚拟机与主机互相访问，不能访问外部（物理网络上的计算机或外部网络，例如 Internet），外部也不能访问“内部”的虚拟机。例如，在图 11-27 中，虚拟机 A11、A12 以及 A 可以互相访问，但不能访问物理网络上的其他计算机。

“专用”虚拟网络只允许虚拟机之间互相访问，与物理主机也不能互相访问。例如，在图 11-27 中，A21、A22、A23 可以互相访问，但不能访问物理主机 A。

在同一个物理主机中，“外部”、“内部”、“专用”虚拟网络，相当于物理网络中的不同的“交换机”，它们之间没有网络关系。例如，在图 11-27 中，虚拟机 A11、A21 不能互相访问，A01、A12 也不能互相访问。除非物理主机启用“路由和远程访问”服务中的“路由器”功能，为这两个网段提供访问服务。

在同一个物理主机中，也可以有多个“外部”、“内部”、“专用”虚拟网络，即使都是“内部”或“专用”虚拟网卡，不同的“内部”虚拟网络之间的虚拟机，也是不能互相访问的，网络关系如图 11-28 所示。

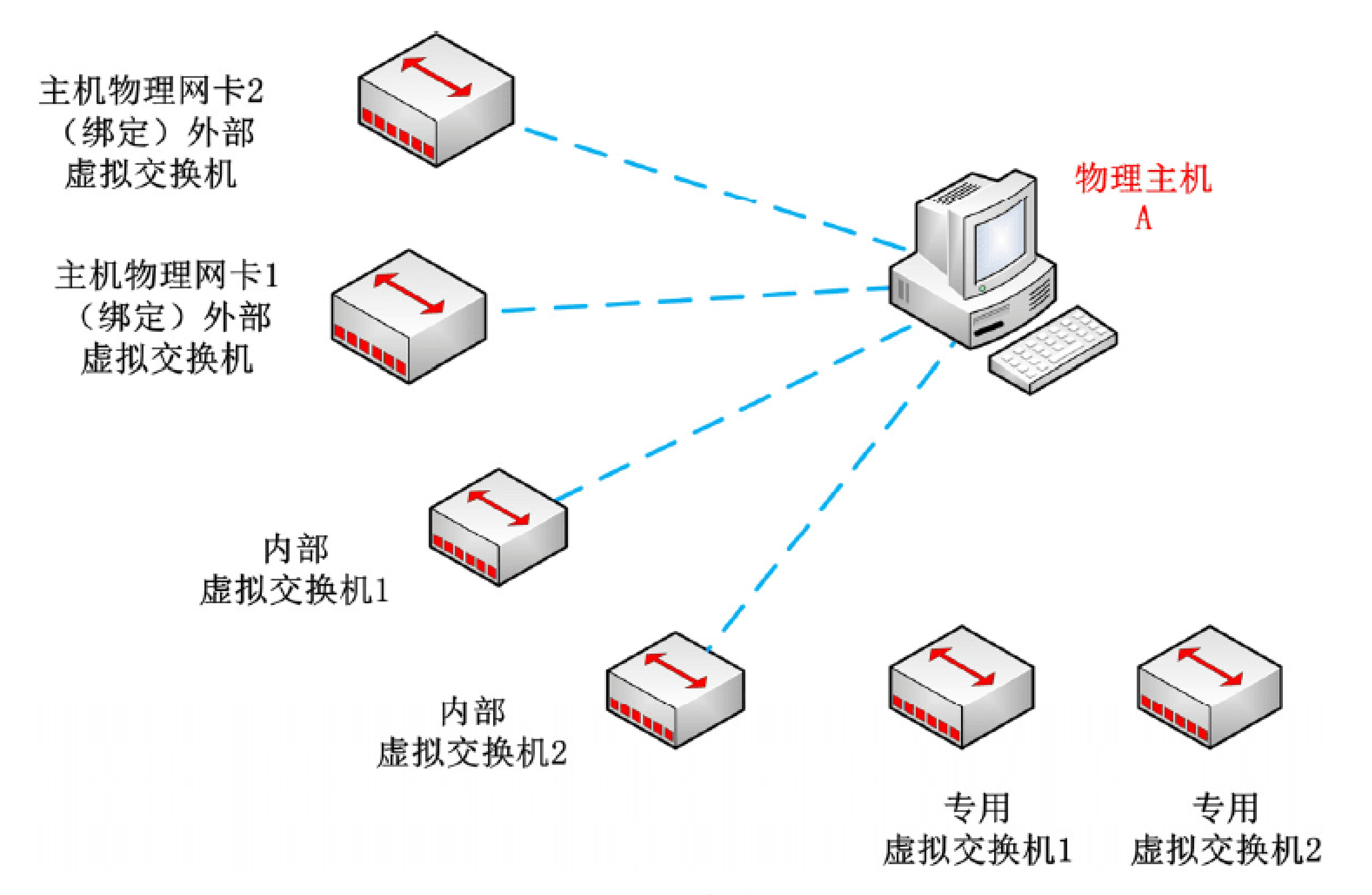


图 11-28　多个虚拟网络

下文通过几个操作，来熟悉 Hyper-V 虚拟网络。

11.7.1　查看物理网卡与虚拟网卡

在 Hyper-V 中，主要是创建“外部”虚拟网络，很少或基本不用“内部”或“专用”虚拟网络，因为 Hyper-V 提供的虚拟机主要是为网络中的其他计算机提供网络服务的。当然，如果只是用 Hyper-V 做实验主机则另当别论。

由于“外部”虚拟网络需要“绑定”到主机的物理网卡，所以，当主机有多个物理网卡时（一般服务器至少有 2 个物理网卡，而像 HP DL380G7 系列的服务器，则集成 4 个网卡），用户要记得，创建的“外部”虚拟网络是绑定到哪一块物理网卡，这样在使用的时候才不至于出错。查看网卡信息的具体操作步骤如下。

01 打开“控制面板→网络和 Internet→网络和共享中心”，单击左侧的“更改适配器设置”链接，如图 11-29 所示。



图 11-29　更改适配器设置

02 在打开的“网络连接”窗口中，以“详细信息”方式查看，然后对每个网卡重新命名，并记下网卡对应的“设备名”，如图 11-30 所示。在本例中，将 2 块物理网卡分别命名为 lan 与 lan2。虽然这 2 个网卡都是 Intel 的网卡，但 lan2 的设备名称中多出“#2”，这表示是第 2 个网卡。而在绑定物理网卡时，则是利用这个设备名进行分辨的。

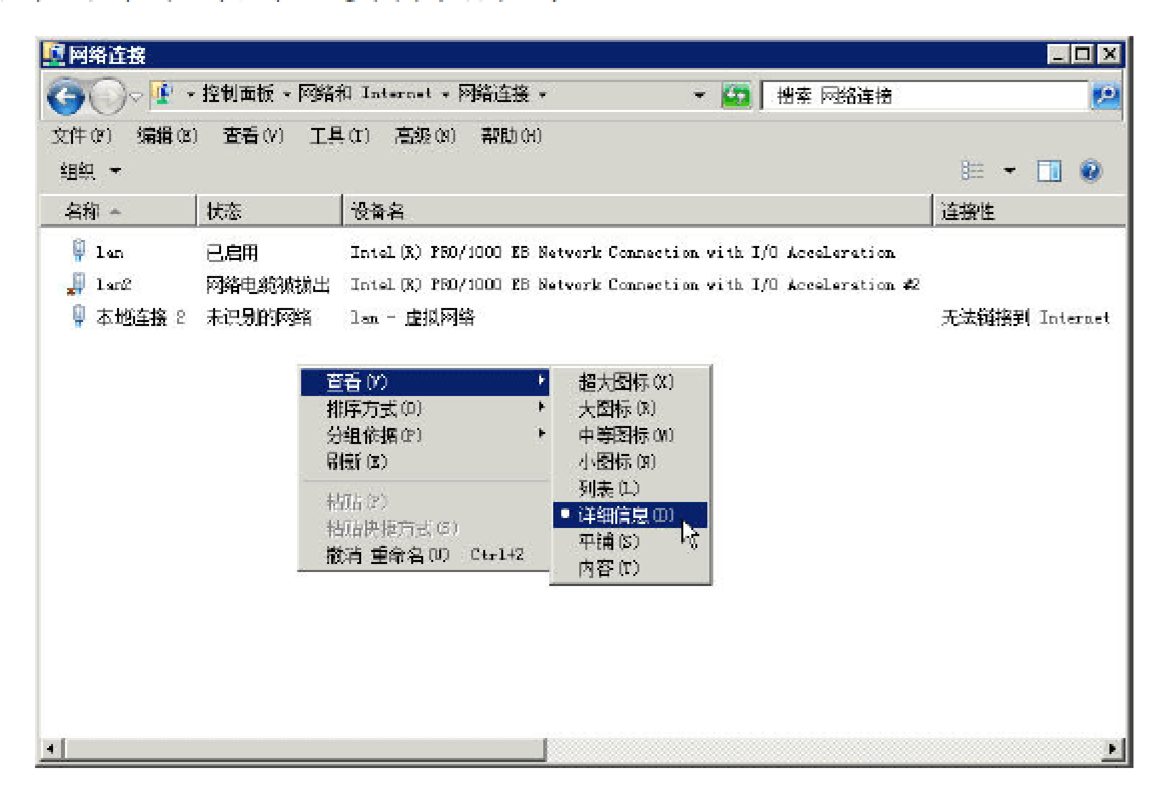


图 11-30　记下网卡设备名

03 在图 11-30 中，还有一个名为“本地连接 2”的虚拟网卡，这个网卡绑定在第 1 个物理网卡上，这是我们安装 Hyper-V 时（如图 11-9 所示），选择的“外部”网卡。

04 用鼠标双击第 1 个物理网卡（网卡重命名为 lan），进入“lan 属性”对话框，在“此连接使用下列项目”选项组中可以看到，当前只绑定了“Microsoft 虚拟网络交换机协议”，如图 11-31 所示。

在创建“外部”虚拟网络时，Hyper-V 将绑定“Microsoft 虚拟网络交换机”到物理网卡，并在创建新的“外部”虚拟网卡时，将绑定的物理网卡原来的 IP 地址、参数等，在虚拟网卡上启用，这样原来物理主机的网络才不会中断。

05 双击“本地连接 2”，在“本地连接 2 状态”的“详细信息”中可以看到，这个虚拟网卡中的信息是原来物理主机网卡的相关参数，如图 11-32 所示。

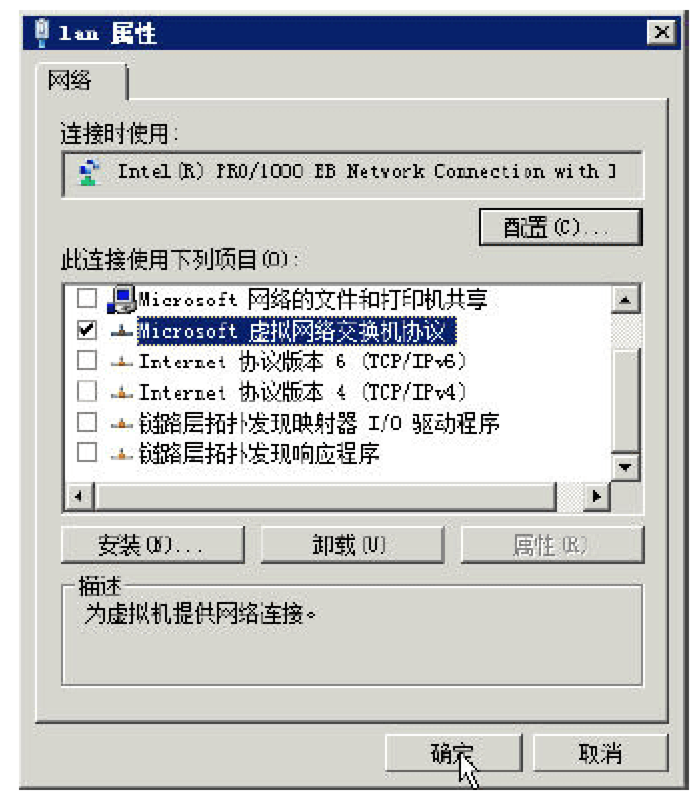


图 11-31　绑定虚拟网络交换机协议

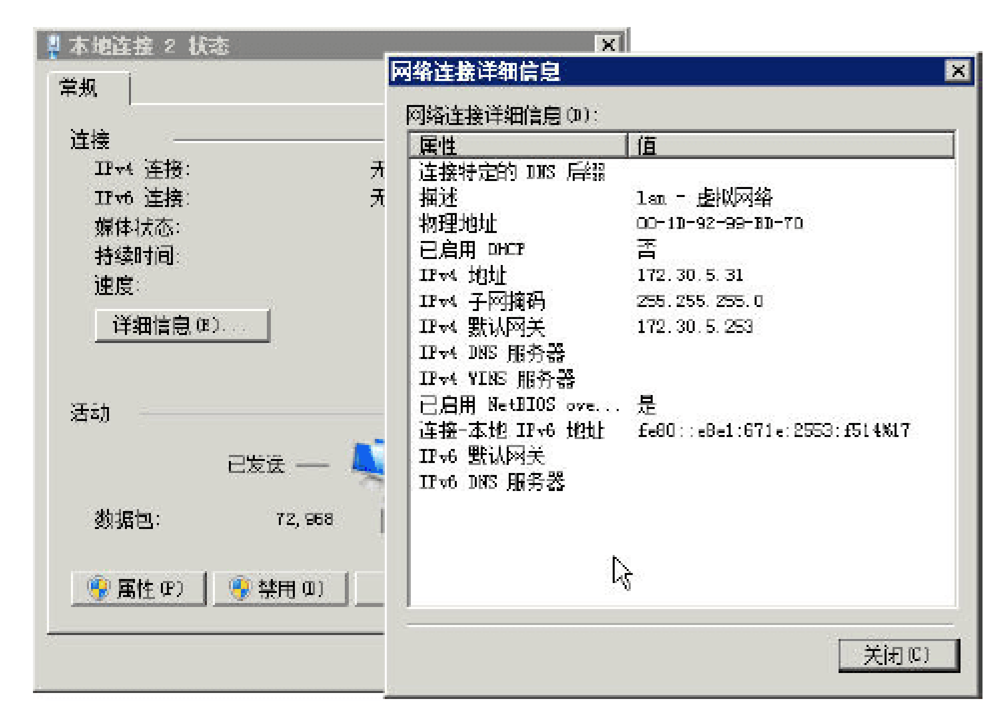


图 11-32　虚拟网卡参数

11.7.2 管理虚拟网络

接下来介绍 Hyper-V 虚拟网络的管理，包括添加、删除、修改虚拟网络。

01 从“管理工具”中选择“Hyper-V 管理器”，如图 11-33 所示，在左侧的任务窗格中选中要管理的 Hyper-V Server 2008 R2 或安装 Hyper-V 功能的 Windows Server 2008，在右侧的“操作”窗格中单击“虚拟网络管理器”。

02 在“虚拟网络管理器”窗口中，在“虚拟网络”列表中选择“lan-虚拟网络”，在右侧的“虚拟网络属性”中可以修改虚拟网络的名称以及说明信息，在“连接类型”选项组中可以修改虚拟网络的连接类型，在“外部”、“仅内部”、“专用虚拟机网络”之间进行选择。如果主要有多个物理网卡并且选中“外部”单选按钮，则可以在下拉列表中，选择使用那块物理网卡进行绑定，绑定的名称则是图 11-30 中所显示的“设备名称”，如图 11-34 所示。

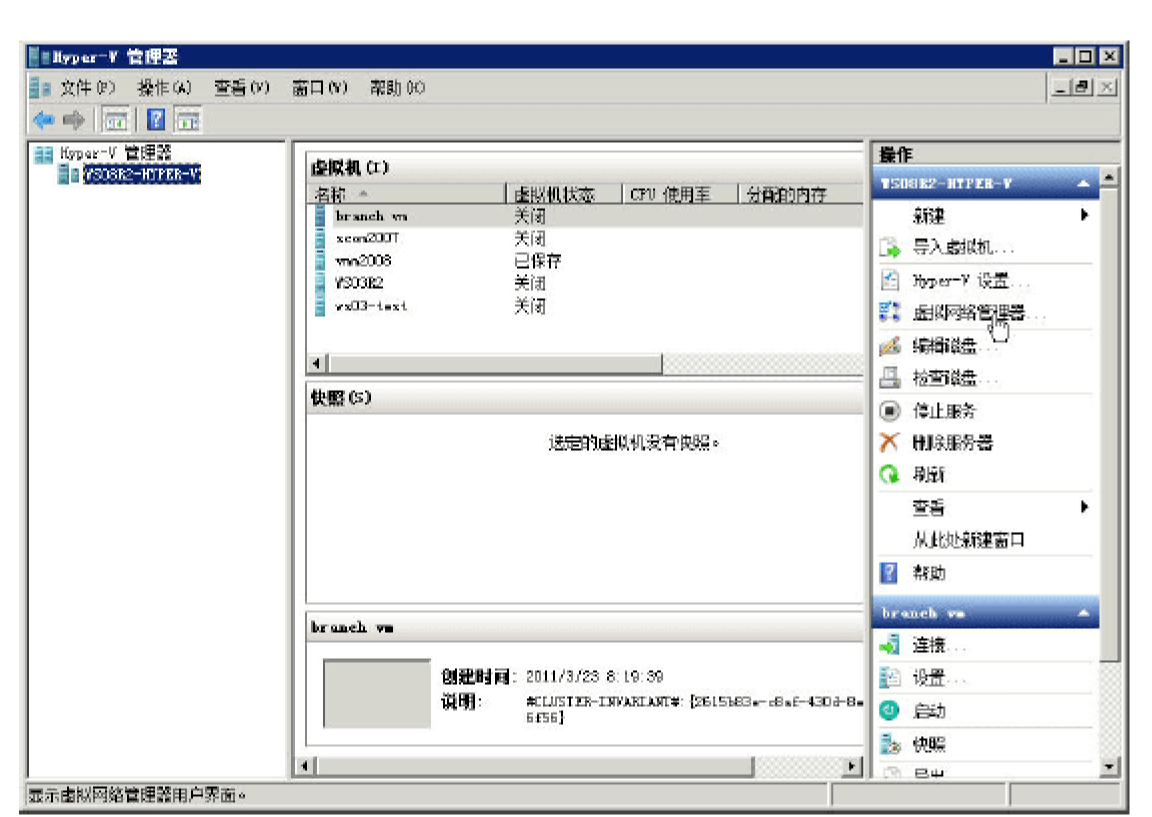


图 11-33 Hyper-V 管理器

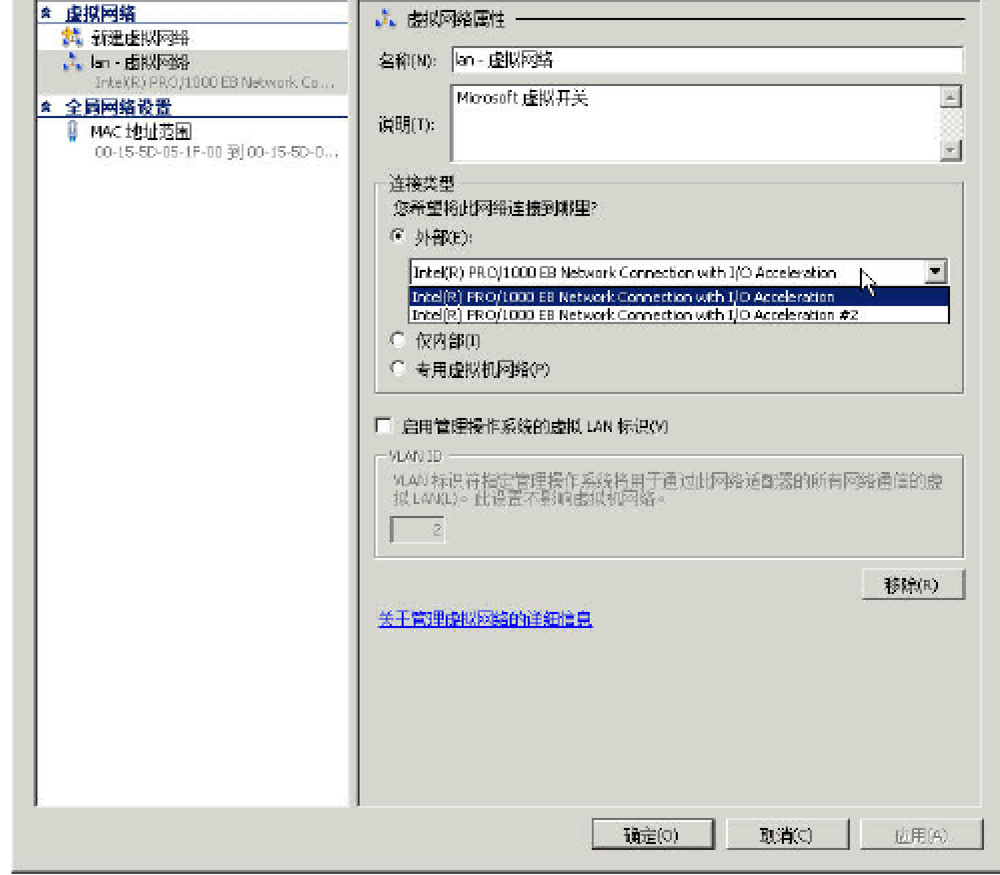


图 11-34 虚拟网络属性

03 如果要删除虚拟网络，可以单击“移除”按钮。

如果要添加虚拟网络，可以按照下面的步骤进行。

01 在“虚拟网络管理器”中，定位到“新建虚拟网络”，在右侧选择要创建的虚拟网络类型——在“外部”、“内部”、“专用”之间选择。选中之后，单击“添加”按钮，如图 11-35 所示。在本例中，选择“内部”。

02 在“名称”文本框中，输入新添加的虚拟网络的名称，一般情况下，添加的名称与网络的属性相关，这样在以后的使用中也容易管理与区分，如图 11-36 所示。在“连接类型”中选择虚拟网络类型，如果要创建多个虚拟网络，也可以用虚拟 LAN 进行标识，可以选中“启用管理操作系统的虚拟 LAN 标识”复选框并为 VLAN 设置 ID。

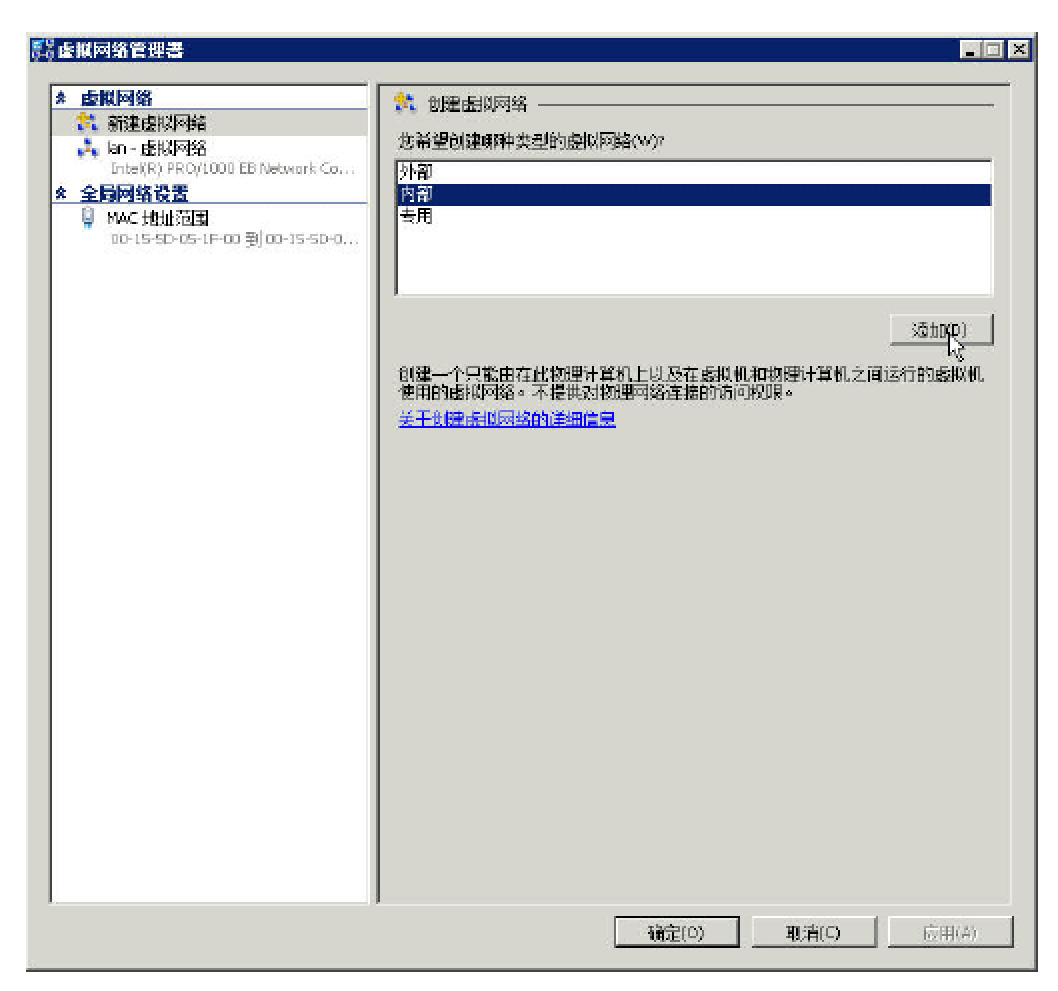


图 11-35　选择要添加的虚拟网络类型

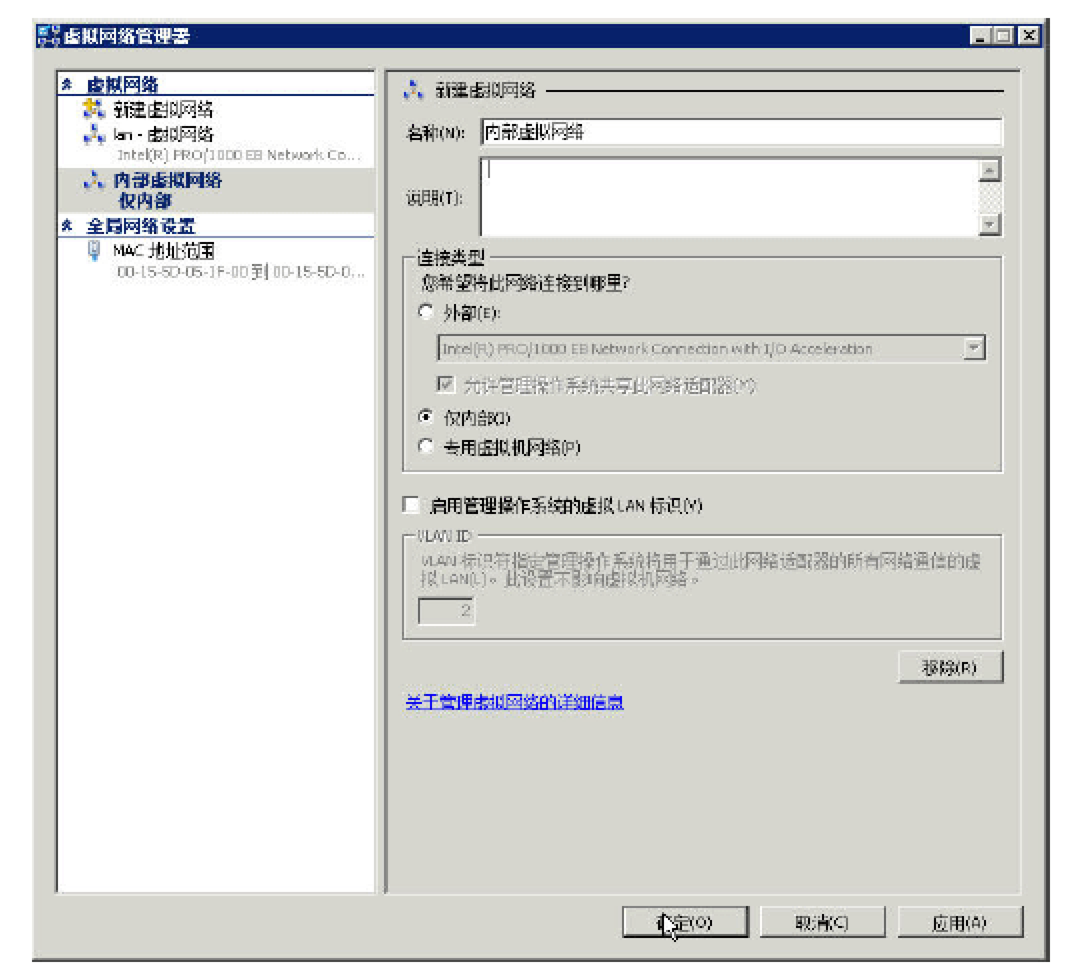
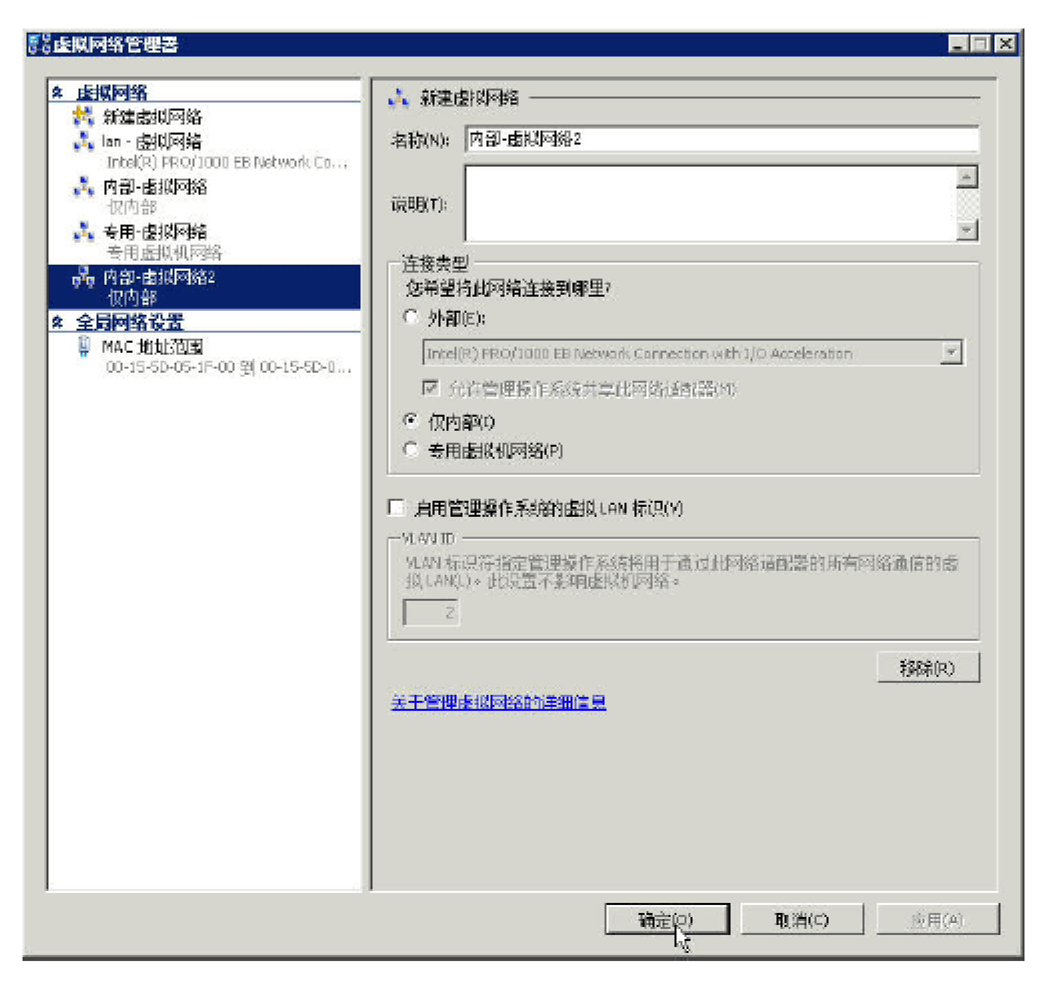


图 11-36　新建虚拟网络

03 设置完成之后，如果只添加这一个虚拟网络，则单击“确定”按钮退出；如果想继续添加虚拟网络，可以单击“应用”按钮，然后单击“新建虚拟网络”，继续添加。

04 接下来，再添加“专用-虚拟网络”、“内部-虚拟网络 2”，添加完成后，单击“确定”按钮，如图 11-37 所示。

05 返回到“网络连接”中可以看到，已经添加了“内部-虚拟网络”与“内部-虚拟网络 2”，而添加的“专用-虚拟网络”则没有在“网络连接”中列出，如图 11-38 所示。这是正确的，因为在前面介绍过，“专用”虚拟网络与主机没有网络连接关系。



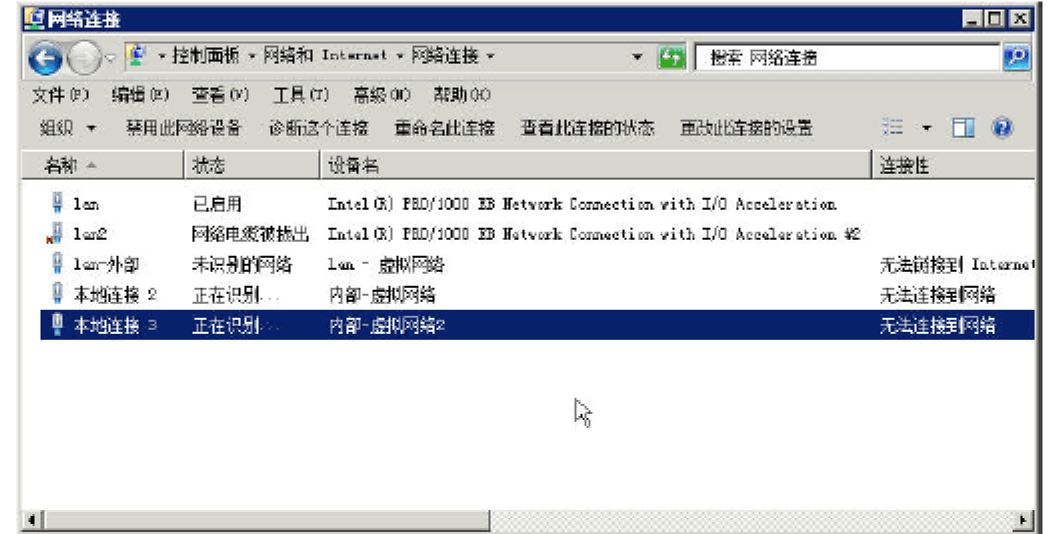


图 11-37　添加多个虚拟网络

图 11-38　网络连接

11.8　Hyper-V 虚拟机管理

在本节中，开始介绍 Hyper-V 虚拟机的管理，包括虚拟机的创建、在虚拟机中安装操作系统

与集成服务（相当于 Hyper-V 虚拟机的驱动）、导出与导入虚拟机、差异磁盘等内容。在学习这些内容之前，我们先对 Hyper-V 进行简单的配置，操作步骤如下。

01 在“Hyper-V 管理器”窗口中单击“Hyper-V 设置”（如图 11-39 所示），进入“Hyper-V 设置”窗口，在右侧“虚拟硬盘”窗格中，单击“浏览”按钮，为虚拟机与虚拟硬盘选择一个默认位置。一般情况下，要选择一个空间比较大的、NTFS 文件系统的目录。在本例中，这个位置是 E:\Hyper-VHDs，如图 11-40 所示。

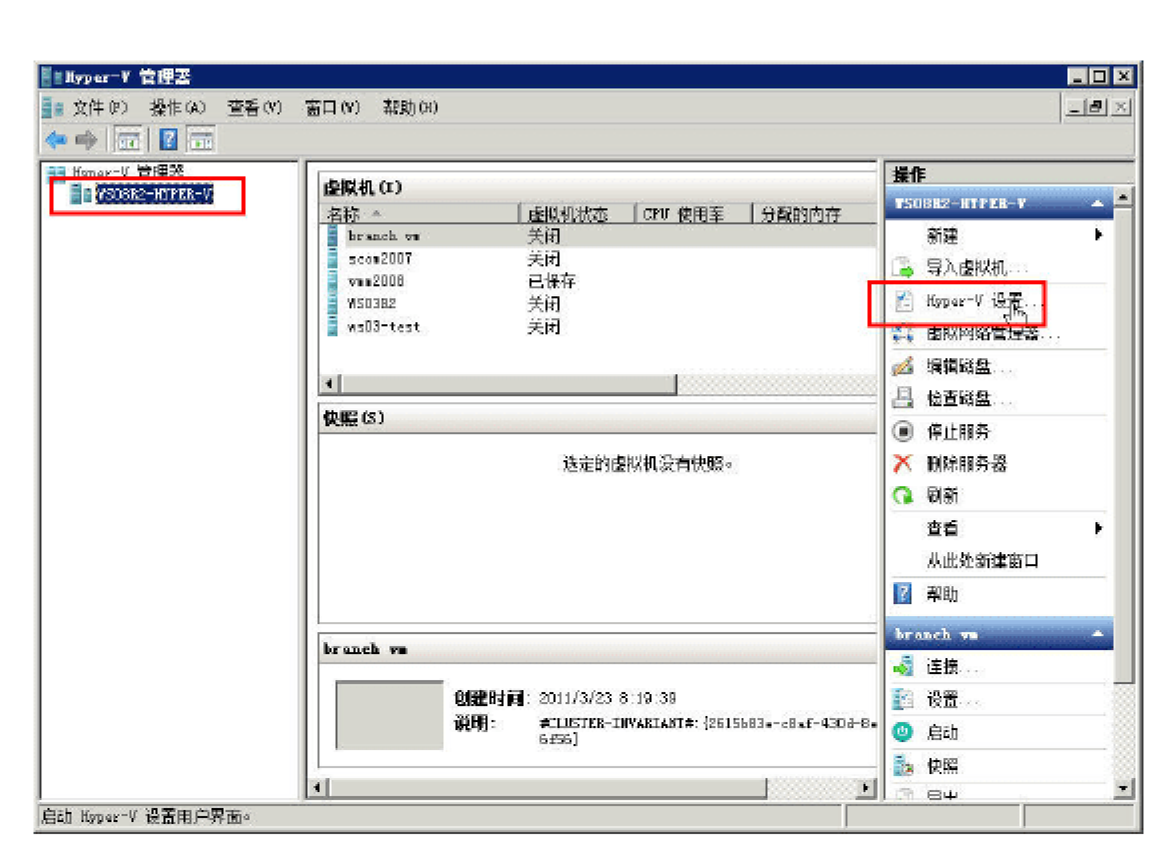


图 11-39　Hyper-V 设置

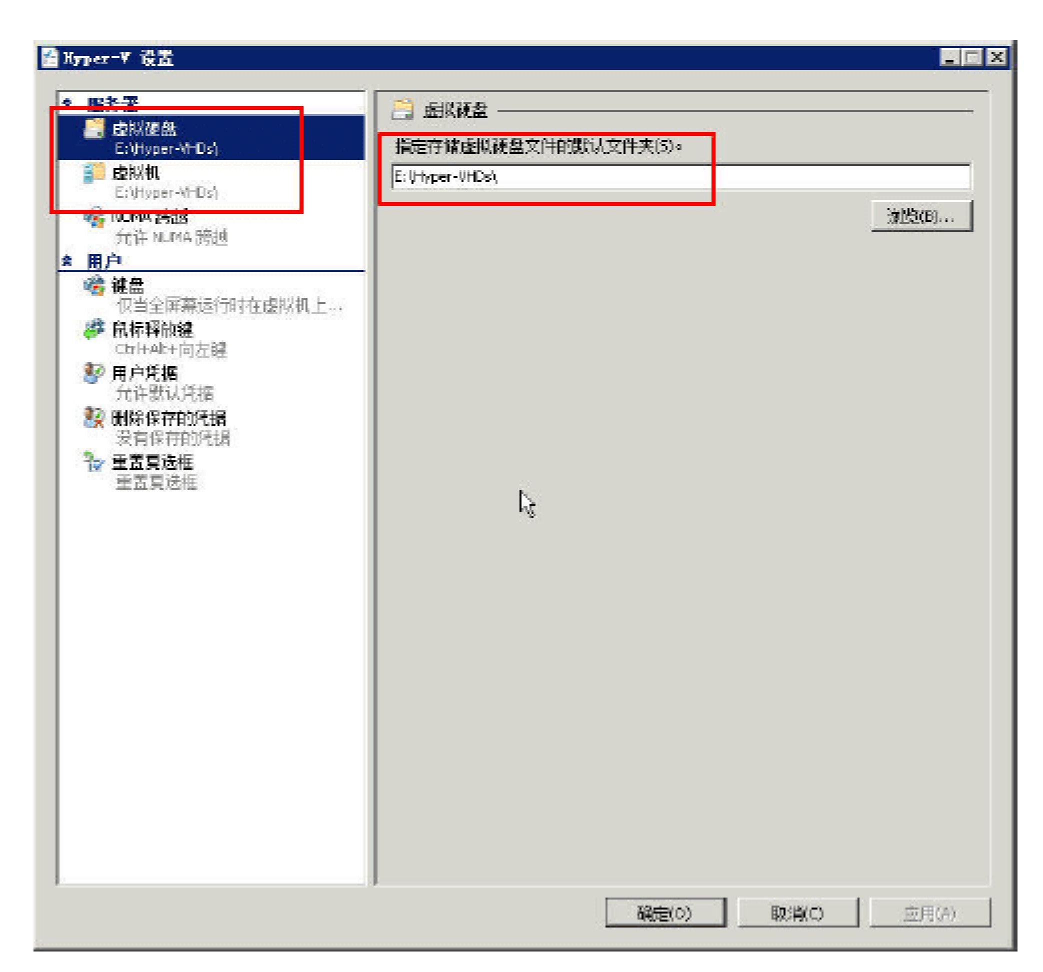


图 11-40　指定虚拟机与虚拟硬盘默认保存位置

02 在“鼠标释放键”处，可以选择从虚拟机返回到主机的热键，默认是“Ctrl+ALT+←”，也可以根据自己的情况进行选择，如图 11-41 所示。

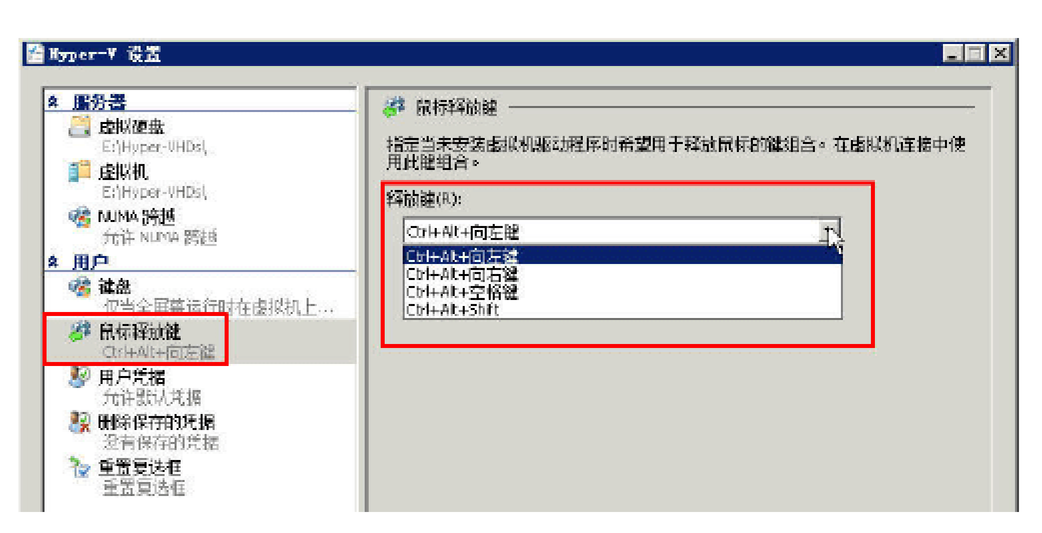


图 11-41　选择鼠标释放键



说 明

如果你的服务器的显卡是 Intel 集成显卡，并且安装了显卡驱动程序，则“Ctrl+Alt+←”与显卡快捷键（将屏幕向左旋转 90°）冲突。为了避免这种情况，可以禁用 Intel 集成显卡的快捷键，或者在上图中，选择其他热键。

在对 Hyper-V 进行简单配置后，我们来介绍虚拟机的管理的内容。

11.8.1　创建模板虚拟机

在 Hyper-V 中创建虚拟机比较简单，以创建一个将要安装 Windows Server 2008 R2 操作系统的

虚拟机为例进行介绍，具体步骤如下。

01 在“Hyper-V 管理器”中，在左侧的任务窗格中，选择要在哪一个主机创建虚拟机，用鼠标右键单击，在弹出的快捷菜单中选择“新建→虚拟机”，如图 11-42 所示。或者在右侧的“操作”窗格中单击“新建→虚拟机”，也可以进入新建虚拟机向导页。

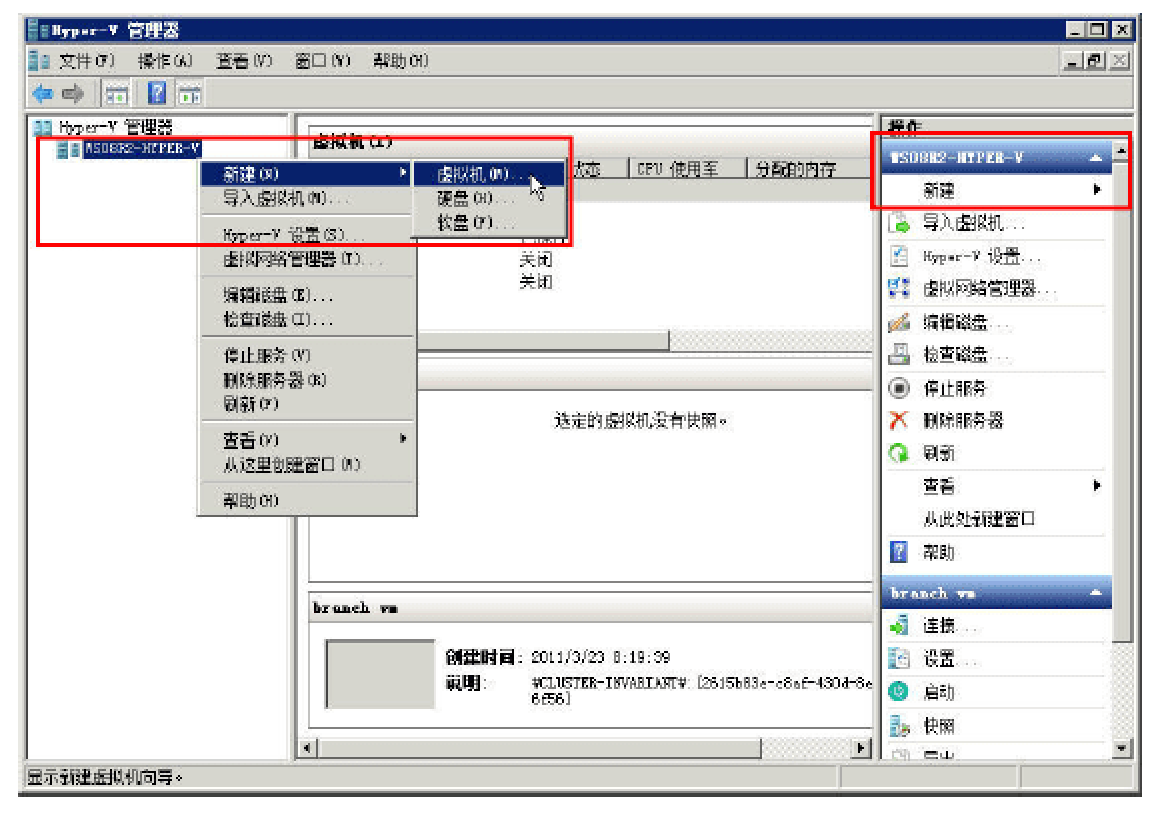


图 11-42　新建虚拟机

02 在“指定名称和位置”对话框中，设置新建虚拟机的名称，在本例中为“ws08r2-temp”，如图 11-43 所示。

03 在“分配内存”对话框中，为虚拟机分配内存的大小，一般情况下，设置为 1024MB（即 1GB）即可，如图 11-44 所示。



图 11-43　指定虚拟机的名称　　　　图 11-44　为虚拟机分配内存

04 在“配置网络”对话框中，为虚拟机选择网卡——选择不同的网卡将连接到不同的虚拟网络。在 Hyper-V 虚拟机中，通常选择连接到物理网络的虚拟网卡，因为 Hyper-V 的服务器一般是对外提供服务的。在本例中选择“lan-虚拟网络”，如图 11-45 所示。在前面的学习中我们知道，这块网卡连接到第 1 块物理网卡。

05 在“连接虚拟硬盘”对话框中，选中“创建虚拟硬盘”单选按钮，“大小”保持默认值 127GB，如图 11-46 所示。

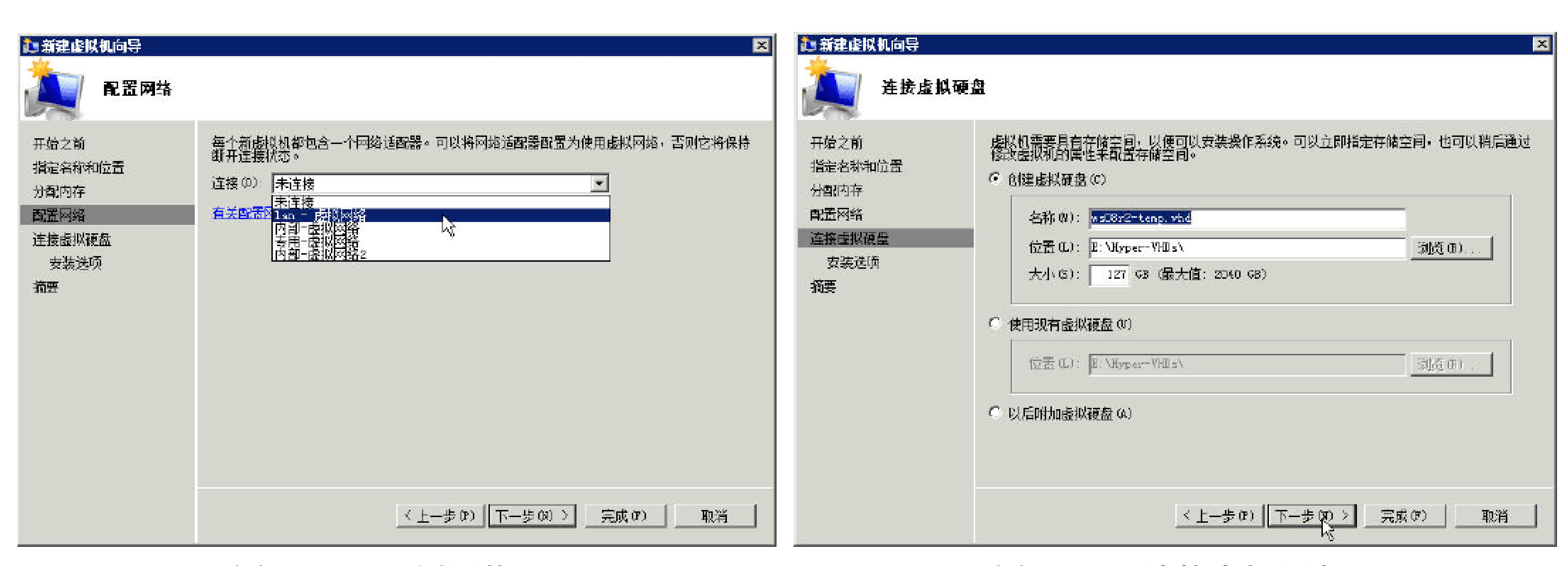


图 11-45　配置网络　　　　图 11-46　连接虚拟硬盘

06 在“安装选项”对话框中，选中“从引导 CD/DVD-ROM 安装操作系统”单选按钮，并选中“映像文件”单选按钮，并浏览选择 Windows Server 2008 R2 With SP1 的光盘镜像，如图 11-47 所示。如果要安装其他的操作系统，可选择对应的操作系统安装镜像。

07 在“正在完成新建虚拟机向导”对话框中，查看创建虚拟机的配置信息，如果需要修改，可单击“上一步”按钮。确认无误后，单击“完成”按钮，如图 11-48 所示。



图 11-47　选择操作系统安装光盘镜像　　　　图 11-48　创建虚拟机向导完成

11.8.2　在虚拟机中安装操作系统

在创建虚拟机之后，接下来开始启动虚拟机并在虚拟机中安装操作系统，安装 Hyper-V 集成服务，主要步骤如下。

01 在“Hyper-V 管理器”窗口中，选中新创建的虚拟机，使用鼠标右击，选择“连接”命令，如图 11-49 所示。

02 连接到虚拟机之后，单击“ ”按钮启动虚拟机，如图 11-50 所示。

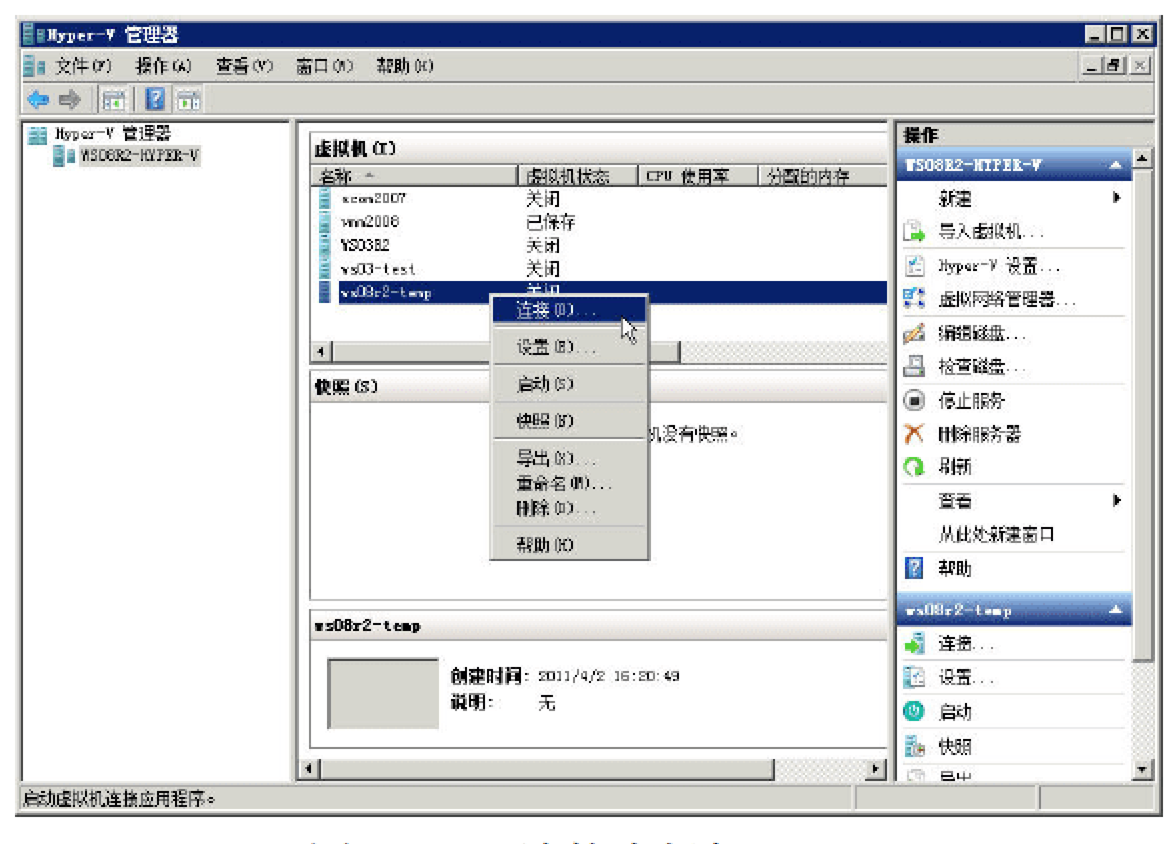


图 11-49　连接虚拟机

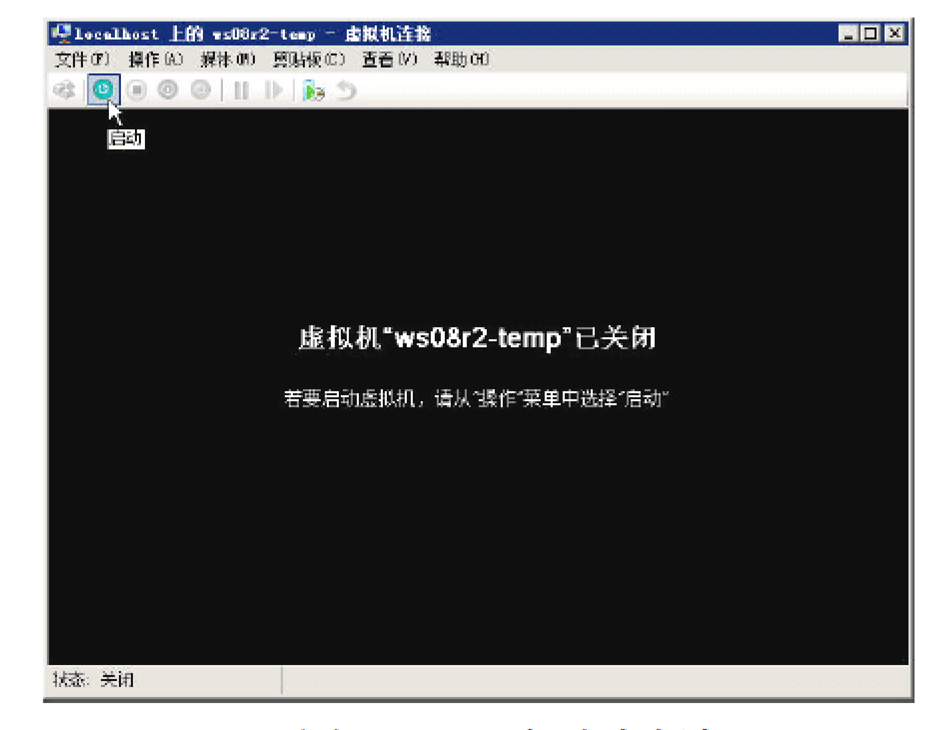


图 11-50　启动虚拟机

03 当虚拟机启动之后，用鼠标在虚拟机窗口中单击，然后就像在物理计算机中一样，在虚拟机中安装操作系统，这些不一一介绍。在本例中，将安装 Windows Server 2008 R2 Enterprise（完全安装），如图 11-51 所示。

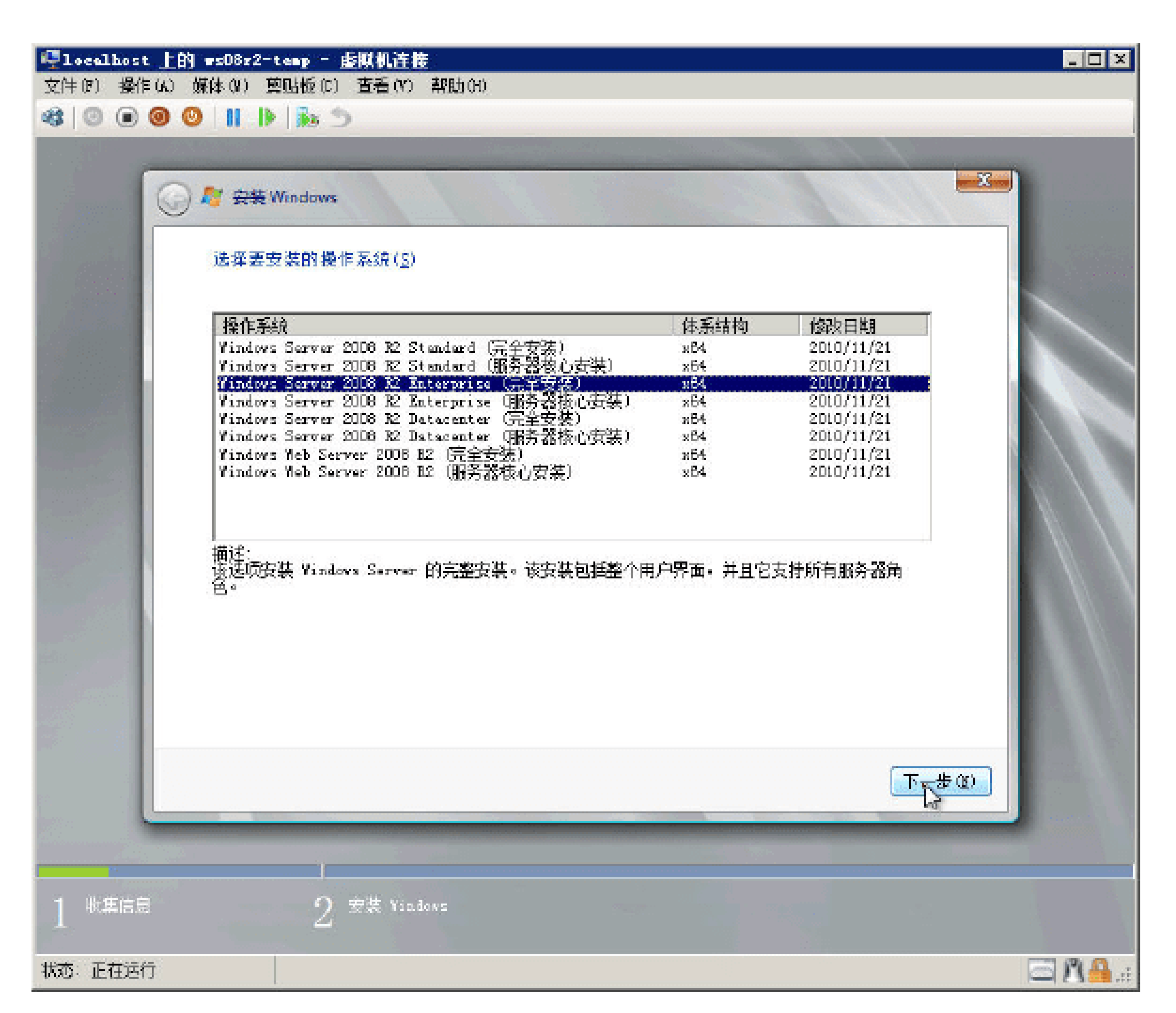


图 11-51　安装 Windows Server 2008 R2 企业版

04 由于 Windows 7、Windows Server 2008 R2 等操作系统已经集成了"Hyper-V 的集成服务"，所以在安装完成之后，不需要安装这些。如果你在虚拟机中安装的是 Windows XP、Windows Server 2003 等操作系统，须单击"操作→插入集成服务安装盘"，然后在虚拟机的"光驱"中运行安装程序并安装 Hyper-V 集成服务。

05 在安装好操作系统之后，对于虚拟机而言，要关闭"屏幕保护程序"，在"控制面板→硬件→电源选项"中，为虚拟机选择"高性能"，并且取消"关闭显示器"的选择，如图 11-52 所示。因为对于虚拟机而言，开启屏幕保护等操作是没有意义的，如果启用这些配置，会占用系统资源。

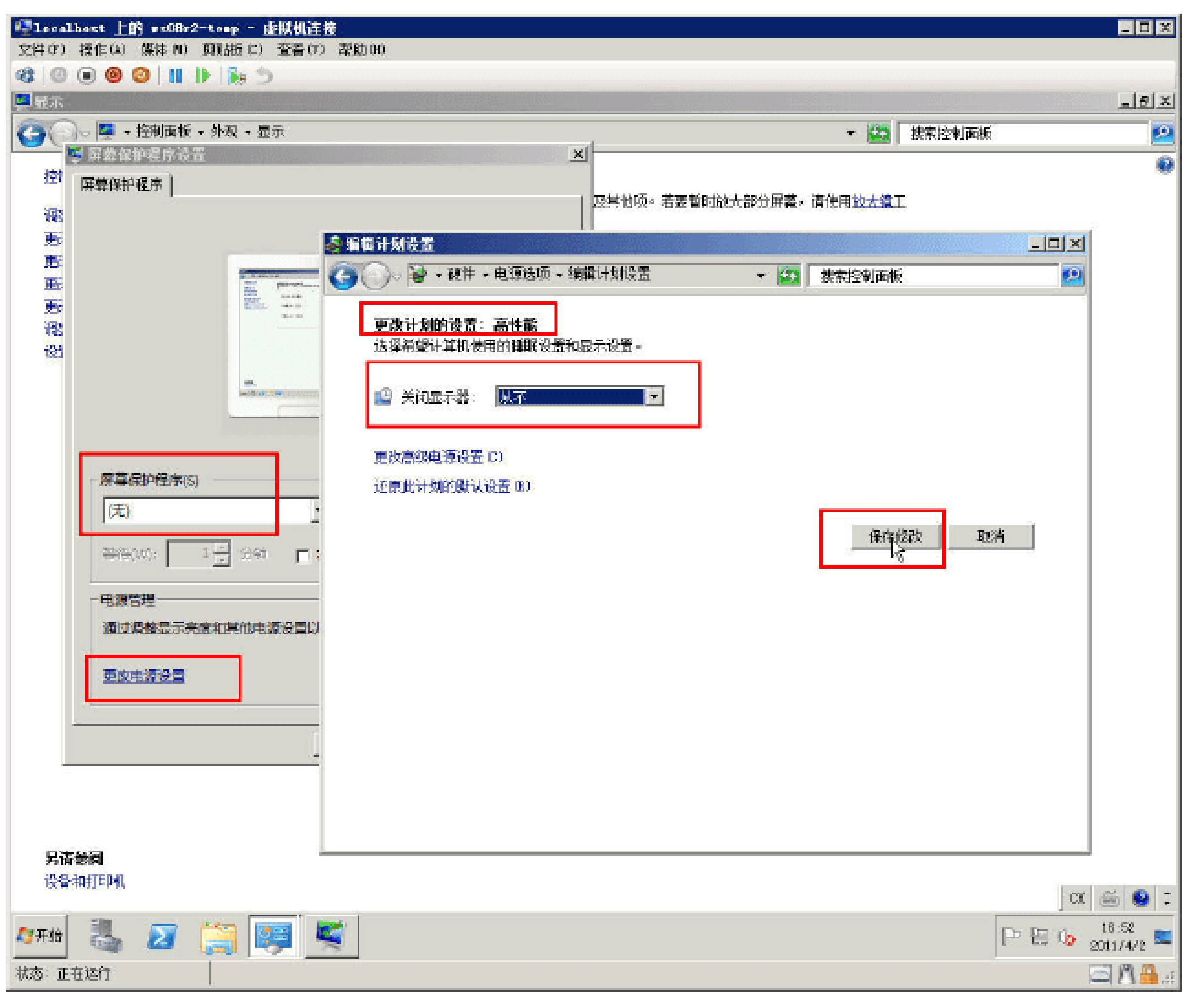


图 11-52 关闭屏幕保护

如果要将这个虚拟机作为模板并“克隆”出多个虚拟机，就要为这台新安装的虚拟机安装最新的补丁，并安装必需的软件，例如压缩解、压缩软件等，安装完成之前，运行 sysprep 程序并关机，以后这台虚拟机将做为“模板”保存并不再使用，主要操作步骤如下。

01 进入命令提示符，在%systemroot%\system32\sysprep 目录中，执行 sysprep 程序，在弹出的“系统准备工具 3.14”对话框中，在“关机选项”下拉列表中选择“关机”，如图 11-53 所示，sysprep 程序运行完成之后将自动关机。

02 当虚拟机关机之后，如图 11-54 所示，继续后面的操作。

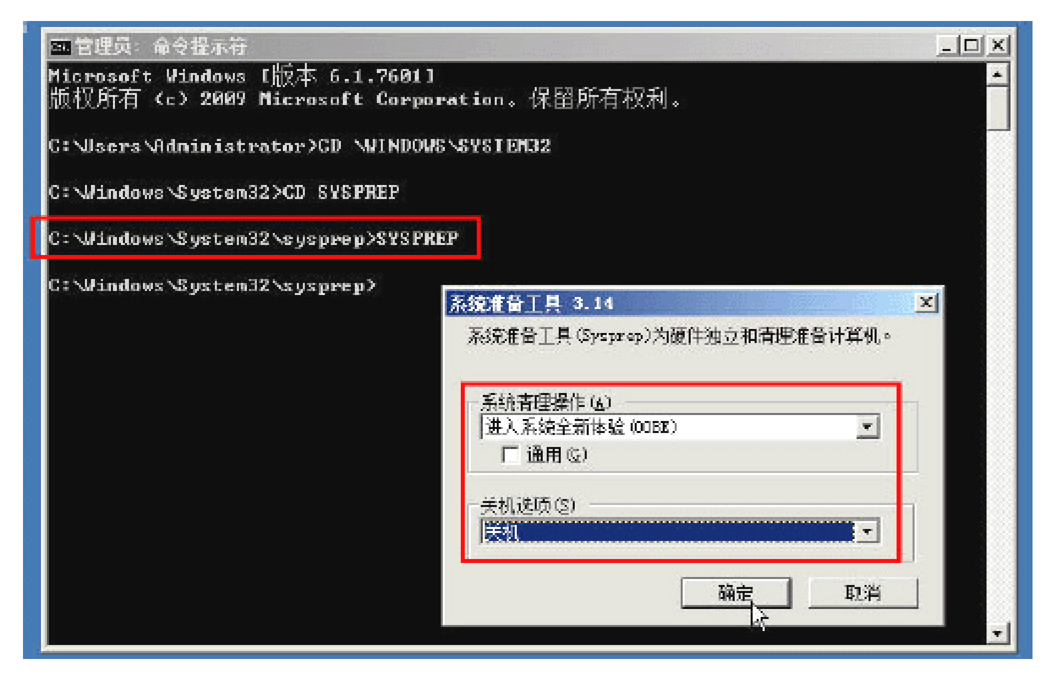


图 11-53 运行系统准备工具

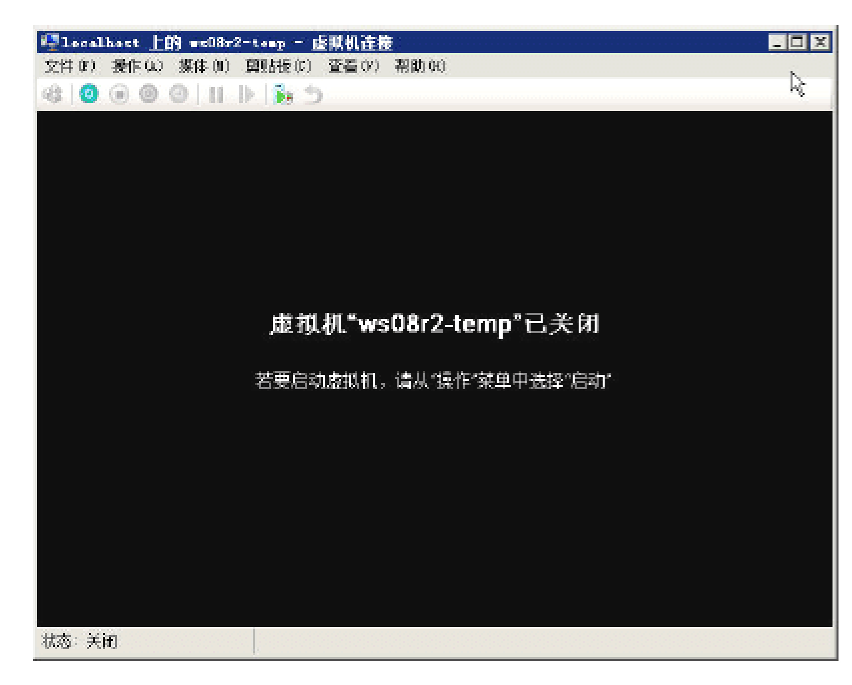


图 11-54 运行 sysprep 完成

11.8.3 导出与导入虚拟机

使用一个设置好的“模板”虚拟机创建多个相同的备份，有两种方法，一种是将选定的虚拟机“导出”然后再改名“导入”，这种方法创建的虚拟机与原虚拟机完全一样，包括占用的硬盘空间大小都相同；另一种是以“模板”虚拟机为基准，使用“差异”磁盘创建多个虚拟机，新创建的虚拟机“依附”模板虚拟机的磁盘，而新虚拟机的改动只反映在新创建的“差异”磁盘中，并占用减小的空间。

对于这两种方式创建的虚拟机，如果“模板”虚拟机被再次启动或删除，使用“导出”再“导入”的虚拟机将不受影响，但使用“差异”磁盘创建的虚拟机将不能启动。

在 Hyper-V 管理器中，导出虚拟机的步骤如下。

01 在“Hyper-V 管理器”窗口中，选择要导出的虚拟机，单击鼠标右键，在弹出的快捷菜单中选择“导出”命令，如图 11-55 所示。

02 在弹出的“导出虚拟机”对话框中，为导出的虚拟机选择一个不同的位置（相对模板虚拟机来说），在此选择 E: \MSVM-VHD，如图 11-56 所示。

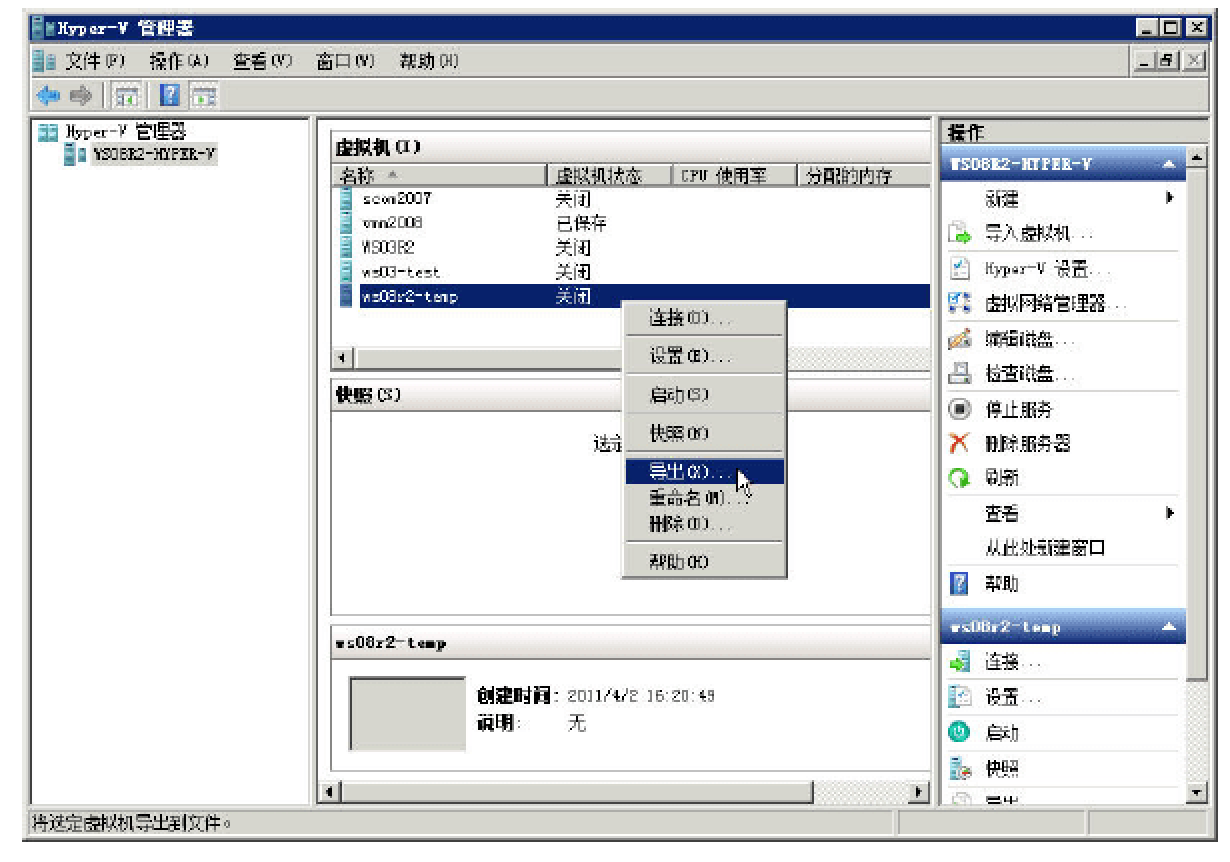


图 11-55　导出虚拟机

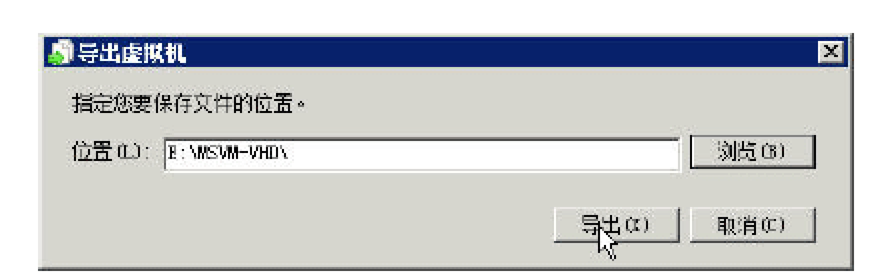


图 11-56　选择导出位置

导出虚拟机完成之后，导入虚拟机的步骤如下。

01 右击要导入虚拟机的 Hyper-V 物理主机，在弹出的快捷菜单中选择“导入虚拟机”命令，如图 11-57 所示。

02 在弹出的“导入虚拟机”对话框中，单击“浏览”按钮，如图 11-58 所示。

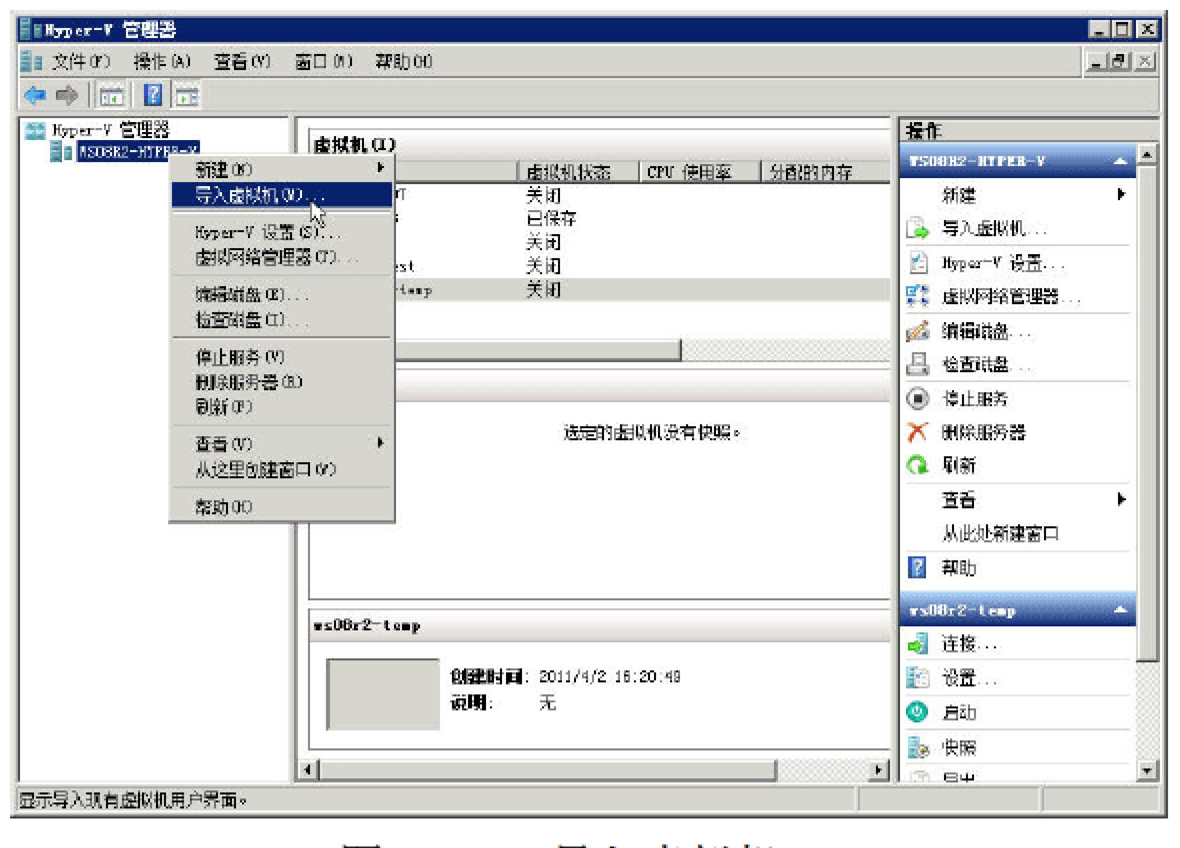


图 11-57　导入虚拟机

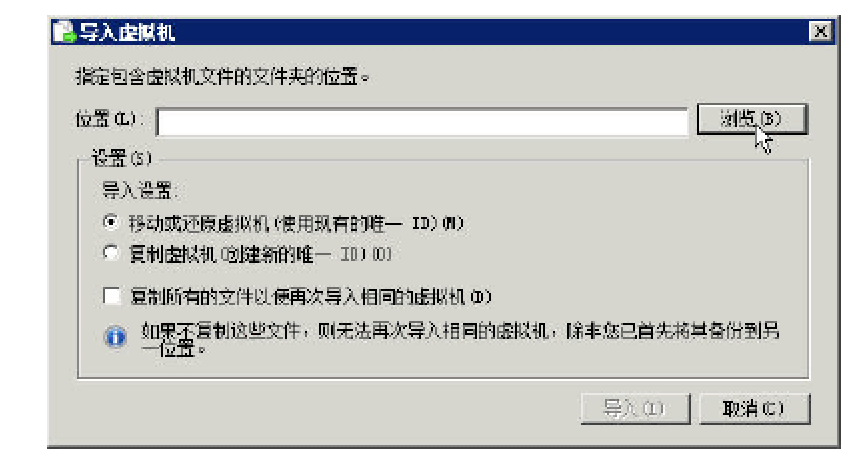


图 11-58　浏览

03 在“选择文件夹”对话框中，选择图 11-56 导出的虚拟机位置，可以看到有一个“ws08r2-temp”的文件夹，这即是导出的虚拟机的目录，在导入之后，用鼠标右击为其重命名，

如图 11-59 所示。

04 在本例中，将其改名为 ws08r2-001，如图 11-60 所示。

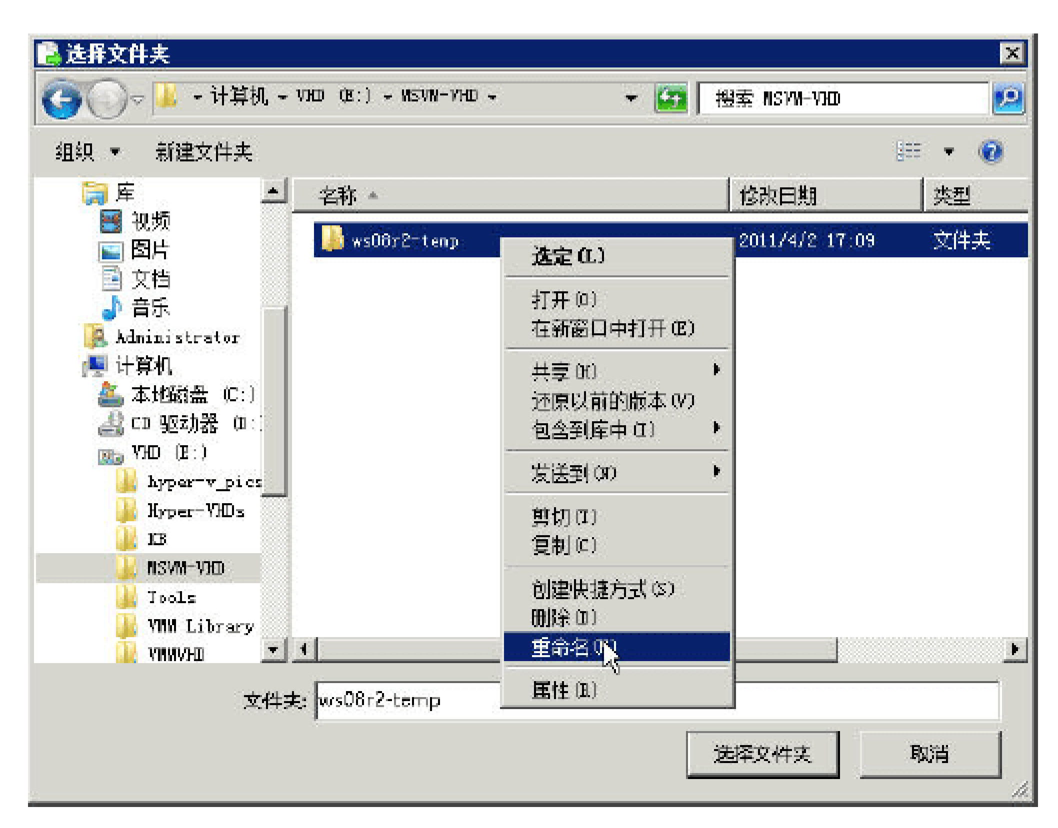


图 11-59 重命名 1

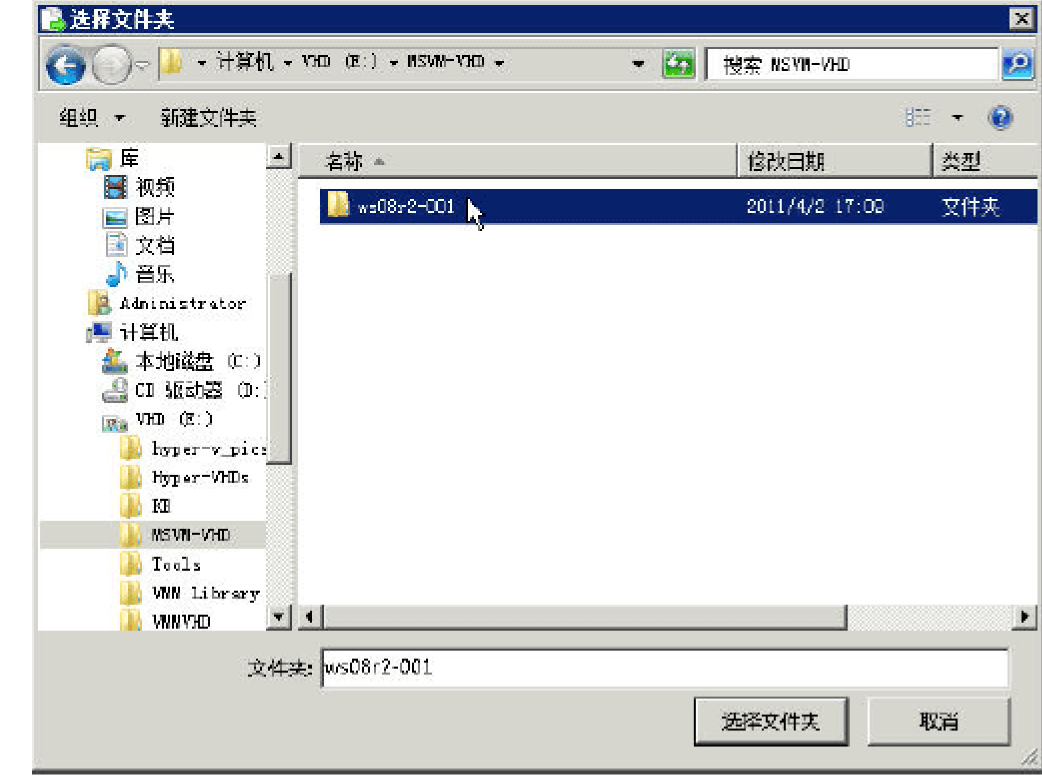


图 11-60 文件夹改名

05 改名之后选择这个文件夹，返回到“导入虚拟机”对话框，在“设置”选项组中选中“复制虚拟机（创建新的唯一 ID）”单选按钮，如图 11-61 所示，然后单击“导入”按钮开始导入。

06 导入完成之后，会弹出警告信息，单击“确定”按钮即可。

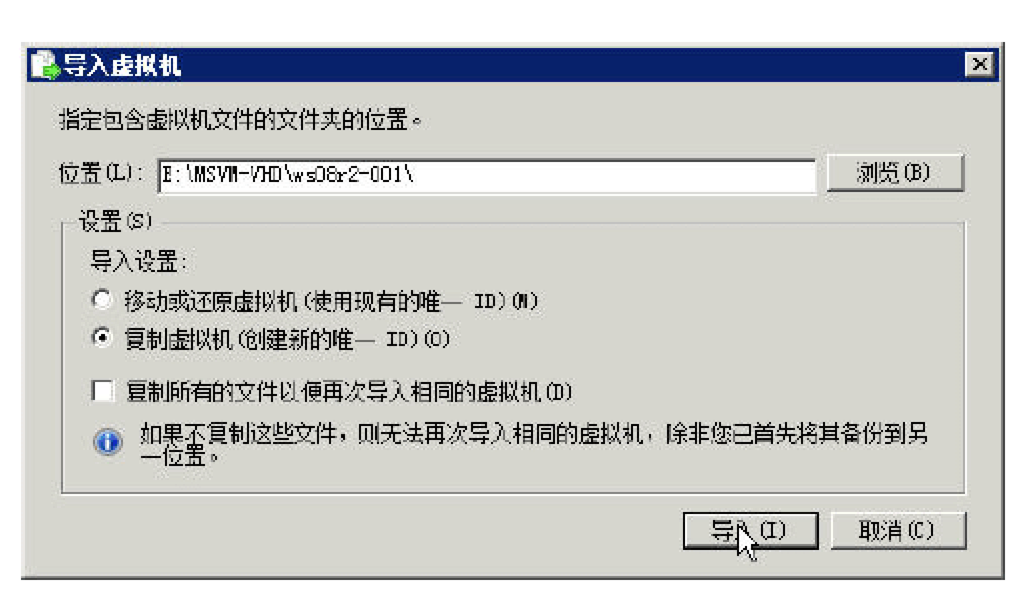


图 11-61 开始导入虚拟机

07 返回到“Hyper-V”管理器窗口后，在“虚拟机”列表框中，可以看到有两个“ws08r2-temp”名称的虚拟机，使用鼠标右键单击选中后一个虚拟机（这个是刚才导入的），在弹出的快捷菜单中选择“重命名”命令，如图 11-62 所示。

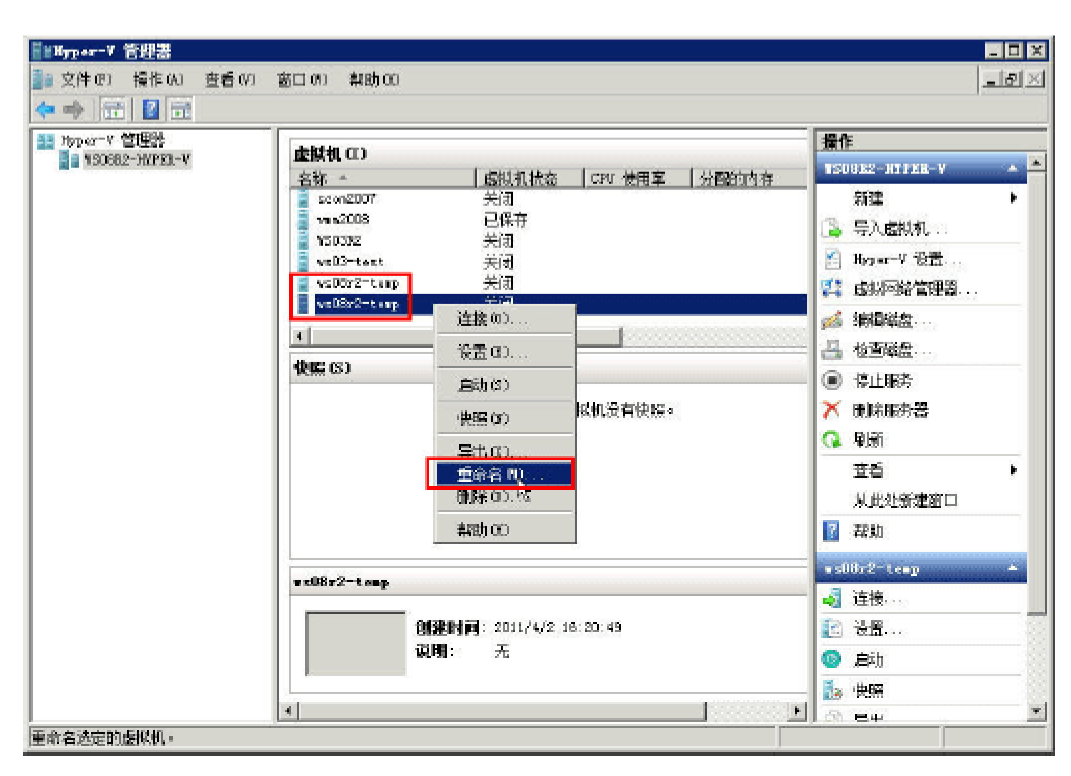


图 11-62 重命名 2

08 在本例中，将新导入的虚拟机重命名为“ws08r2-001”，如图 11-63 所示。

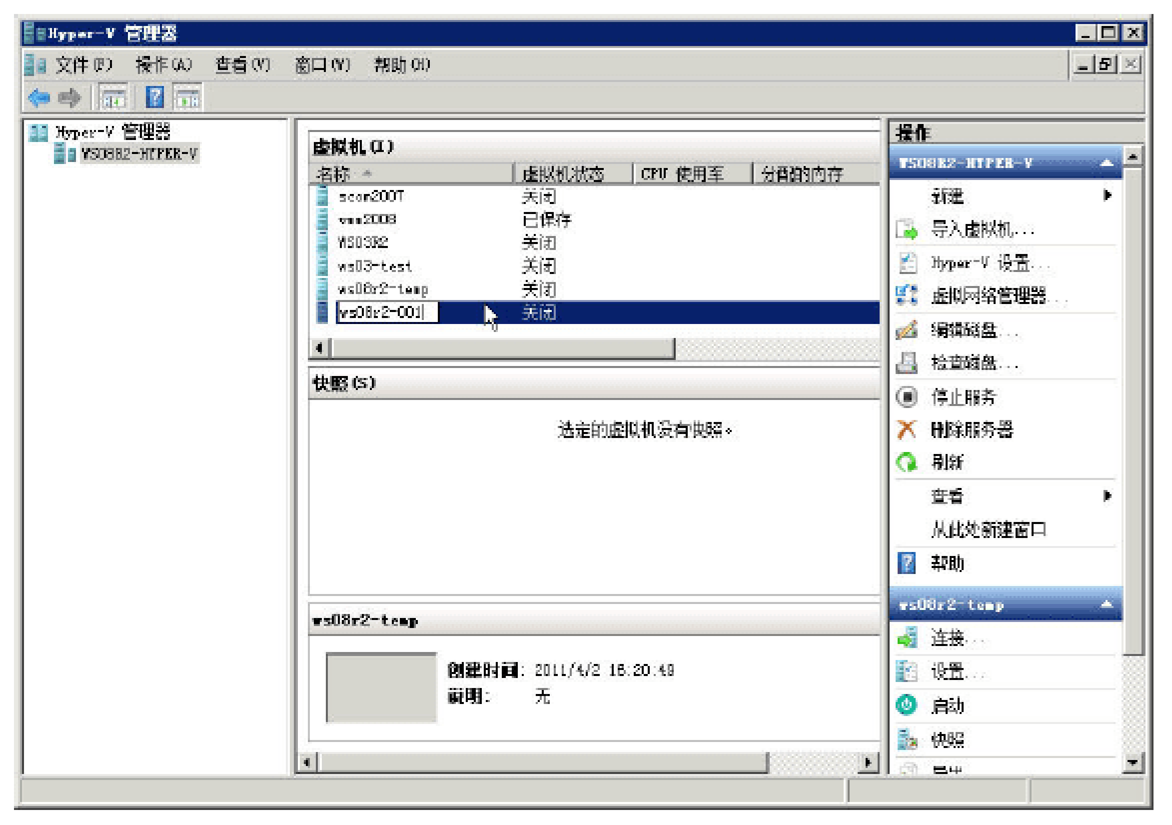


图 11-63　重命名虚拟机

然后选中 ws08r2-001 虚拟机，单击鼠标右键在弹出的快捷菜单中选择“设置”命令，弹出“ws08r2-001 的设置”窗口，在“硬盘驱动器”的右侧单击“检查”按钮，可以看到当前导入的虚拟机的磁盘文件、保存位置、磁盘（使用）大小及磁盘的最大值，如图 11-64 所示。

然后再检查 ws08r2-temp“模板”虚拟机的磁盘的大小，如图 11-65 所示，发现与 ws08r2-001 的大小一致。



图 11-64　检查磁盘大小



图 11-65　检查模板虚拟机的磁盘大小

接下来，学习使用“差异”磁盘创建多个相同虚拟机的方法，为了避免“模板”虚拟机被误用导致新创建的虚拟机不能使用，须在“Hyper-V 管理器”中删除模板虚拟机，如图 11-66 所示。



说 明

在“Hyper-V 管理器”中删除虚拟机时，这只是在“虚拟机”列表中删除，并不是真正地从硬盘中删除虚拟机硬盘文件。

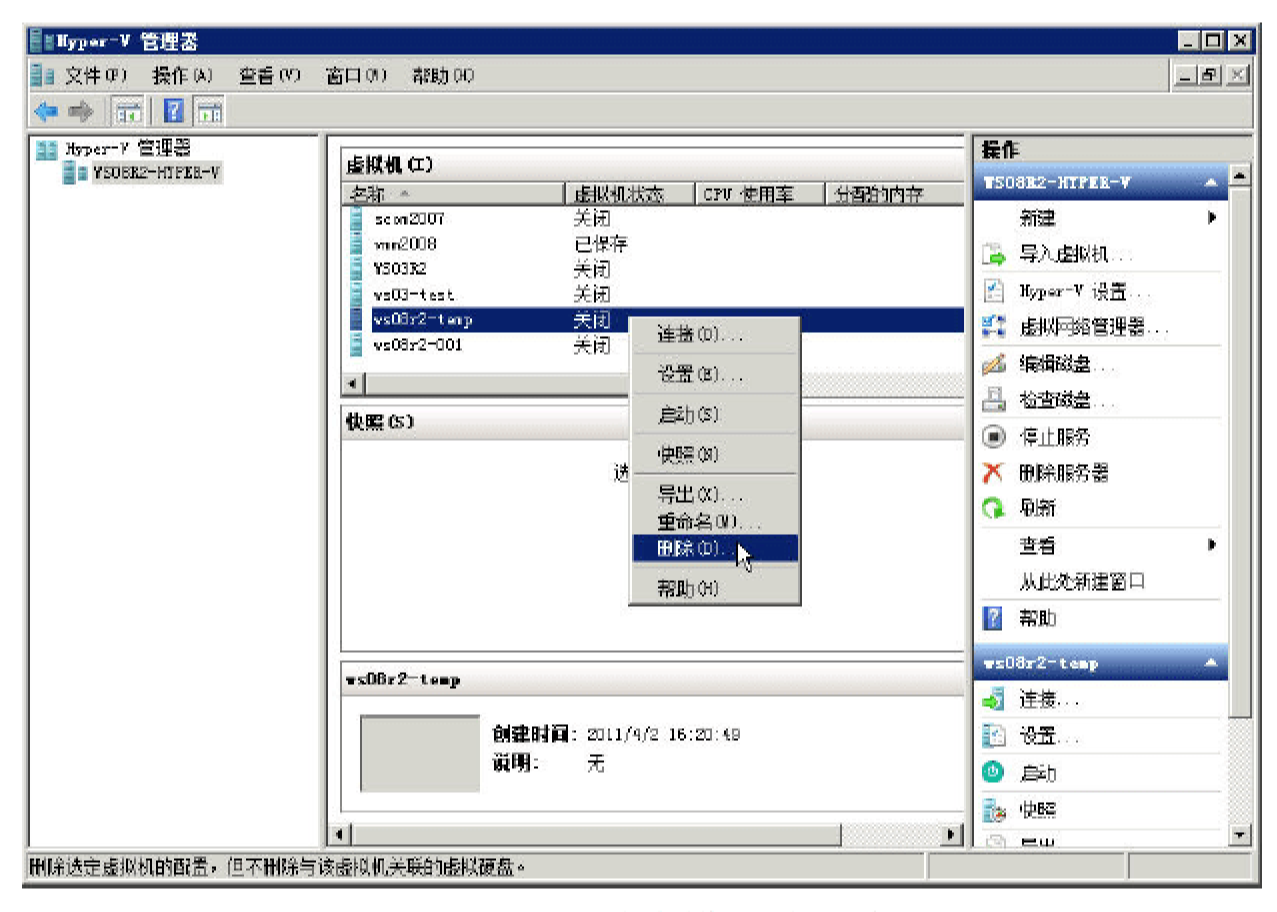


图 11-66 删除模板虚拟机

11.8.4 使用差异磁盘

在下面的步骤中，我们将介绍在虚拟机中使用差异磁盘的方法。首先创建一个虚拟机，并在创建虚拟机时选择“不创建磁盘”，在创建虚拟机完成之后再手动添加磁盘，并在添加磁盘向导中选择使用差异磁盘。主要步骤如下。

01 在“Hyper-V 管理器”中，选择“新建→虚拟机”命令，如图 11-67 所示。

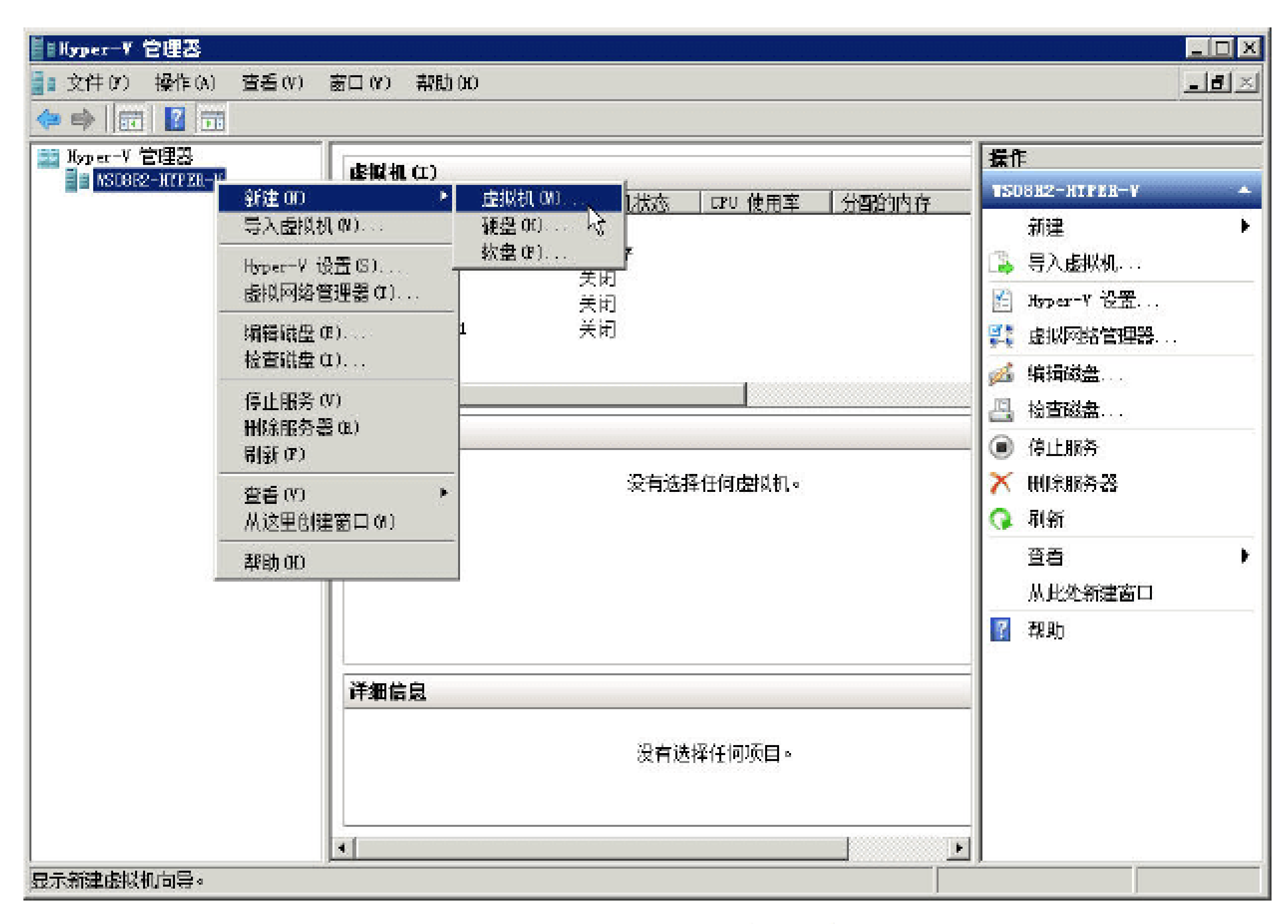


图 11-67 新建虚拟机

02 在“指定名称和位置”对话框中，指定虚拟机的名称为“WS08R2-002”，如图 11-68 所示。

03 在“连接虚拟硬盘”对话框中，选中“以后附加虚拟硬盘”单选按钮，如图 11-69 所示。

04 创建完虚拟机之后，进入虚拟机的设置页面，在“硬件→IDE 控制器 0”处，在右侧选择“硬盘驱动器”，然后单击“添加”按钮，如图 11-70 所示。

05 在“硬盘驱动器”窗格中，单击“新建”按钮，如图 11-71 所示。

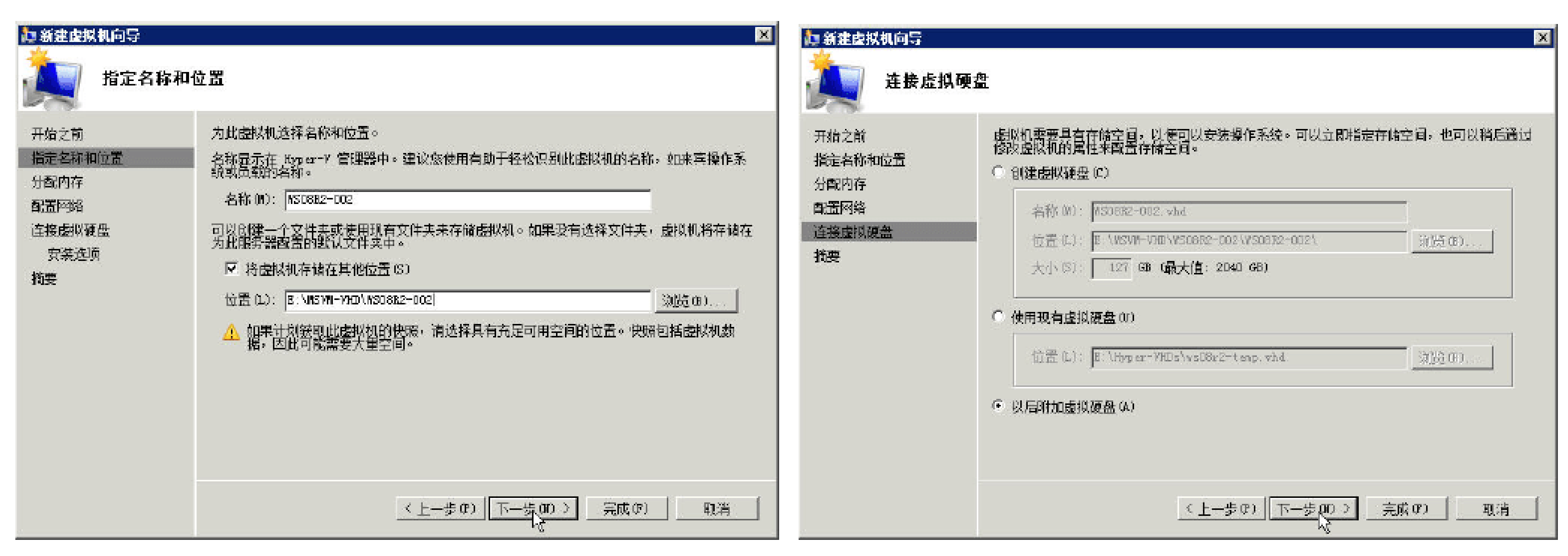


图 11-68　指定虚拟机名称　　图 11-69　以后附加虚拟硬盘

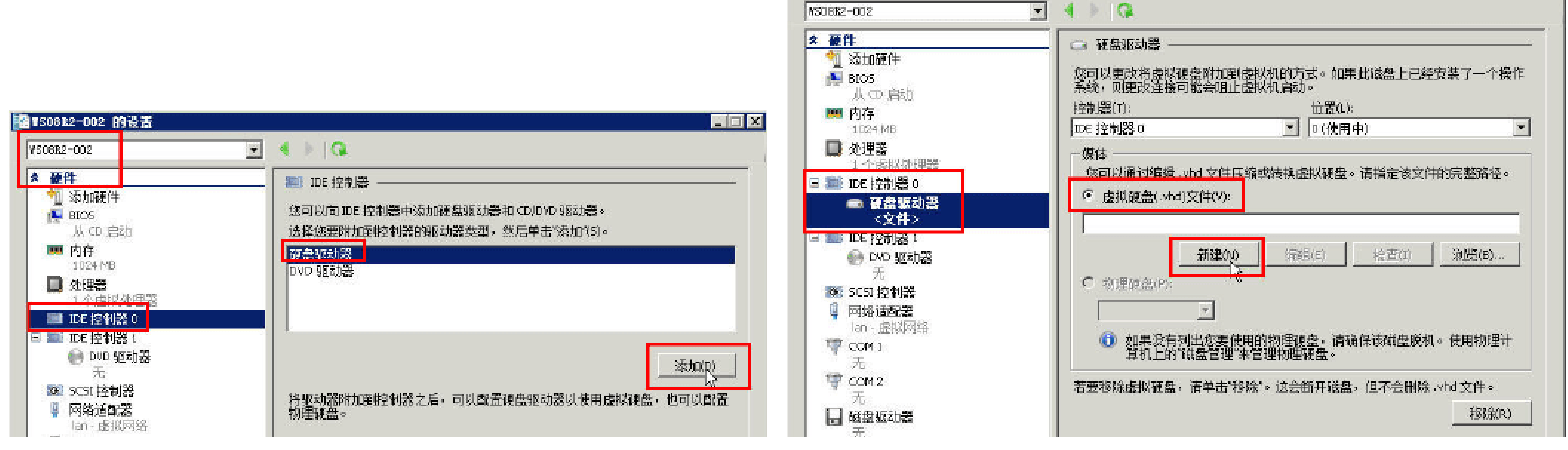


图 11-70　添加磁盘　　图 11-71　新建磁盘

06 在“选择磁盘类型”对话框中，选中“差异”单选按钮，如图 11-72 所示。

07 在“指定名称和位置”对话框中，为新建的虚拟硬盘指定文件名及保存位置，如图 11-73 所示。

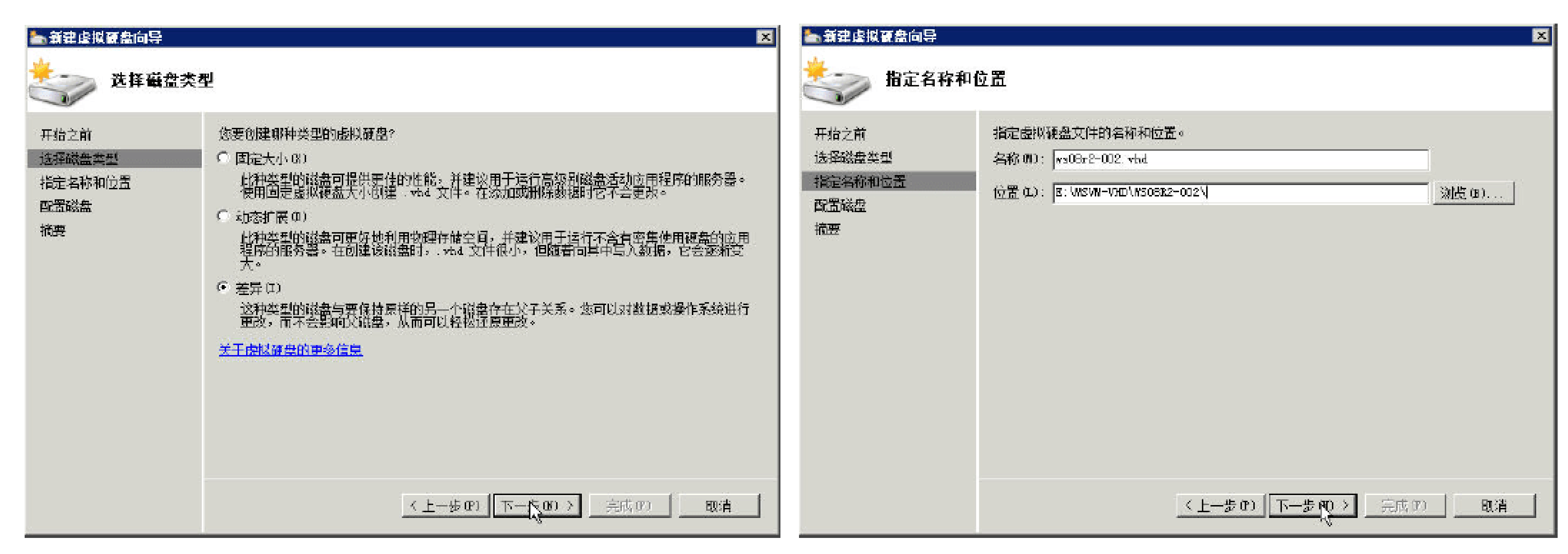


图 11-72　差异磁盘　　图 11-73　指定虚拟硬盘名称和保存位置

08 在“配置磁盘”对话框中，为新的差异虚拟硬盘指定用作父硬盘的虚拟硬盘，在此选择模板虚拟机的虚拟硬盘，在本例中保存为 E:\Hyper-v-VHDs\ws08r2-temp.vhd，如图 11-74 所示。

09 在“正在完成新建虚拟硬盘向导”对话框中，单击“完成”按钮，如图 11-75 所示。



图 11-74　选择父硬盘　　　　图 11-75　完成虚拟硬盘向导

10 返回到虚拟机设置对话框，可以看到，已经创建了虚拟硬盘，如图 11-76 所示。单击“确定”按钮返回到 Hyper-V 管理器。

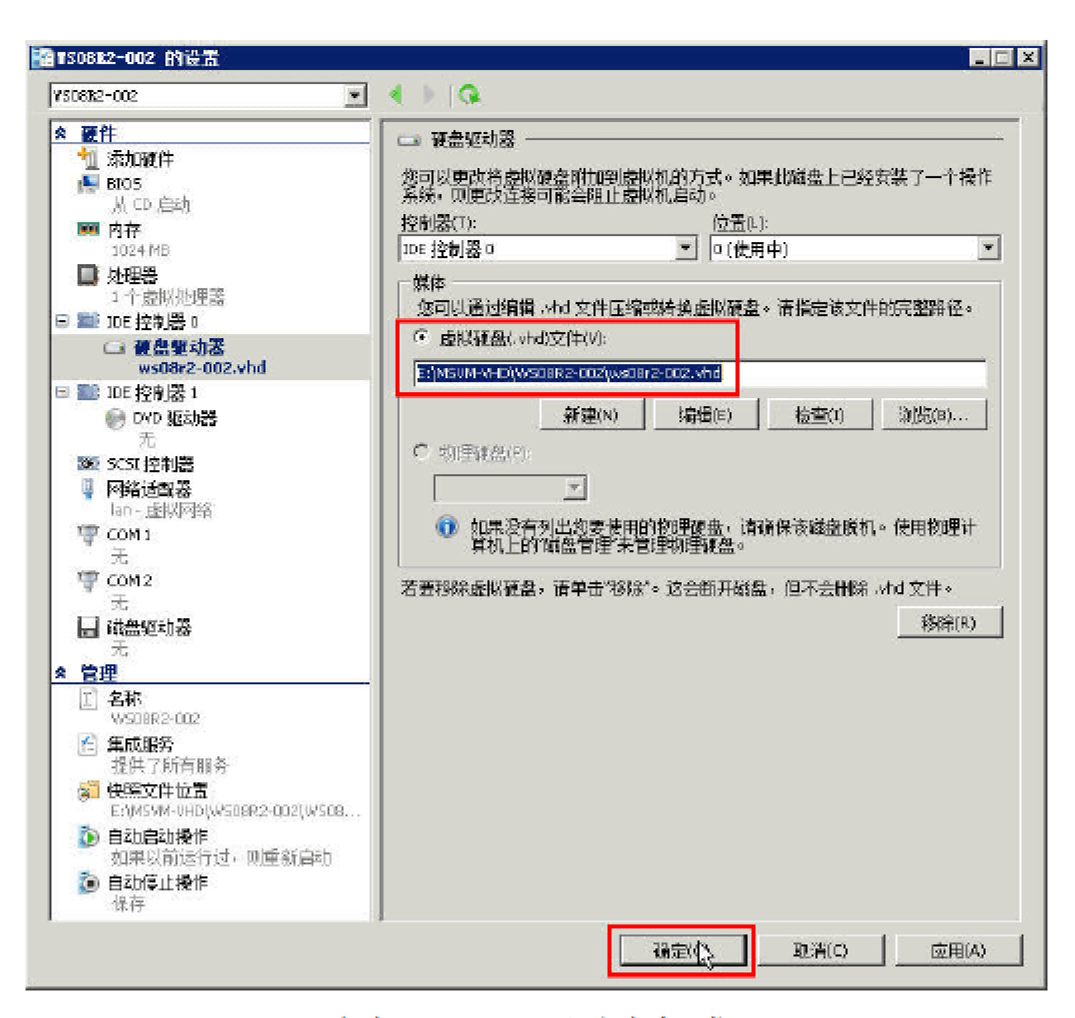


图 11-76　配置完成

11.8.5　启动使用差异磁盘虚拟机

返回到 Hyper-V 管理器之后，启动使用差异磁盘的虚拟机，由于模板虚拟机（父硬盘）在关机之前运行了 sysprep 程序，所以，sysprep 程序会在第 1 次启动虚拟机时，对系统进行重新配置并生成新的 SID，主要步骤如下。

01 首先会出现“安装程序正在为首次使用计算机做准备”的提示，如图 11-77 所示。

02 在“设置 Windows”对话框中，选择国家或地区、时间和货币、键盘布局，如图 11-78 所示。

03 在“输入您的 Windows 产品密钥”对话框中，输入新的 Windows 产品密钥，如果没有，可以单击“跳过”按钮，如图 11-79 所示。

04 在第 1 次进入系统之后，必须修改密码，如图 11-80 所示。

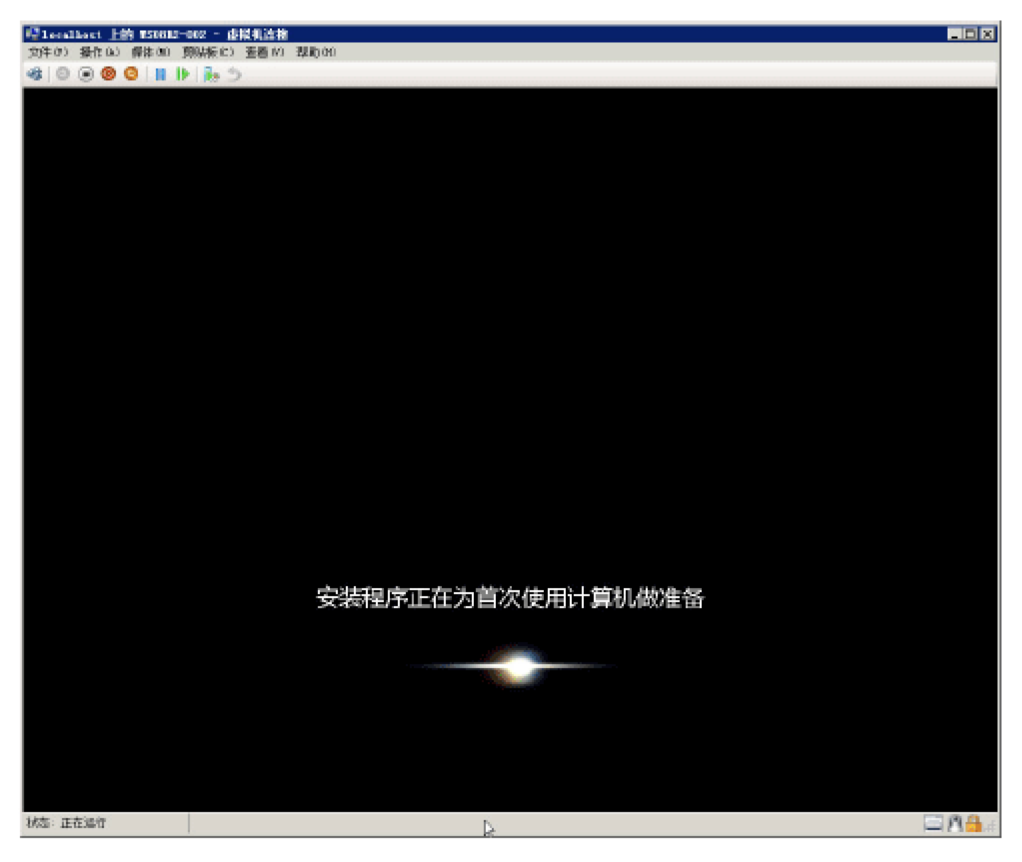


图 11-77　为首次使用计算机做准备

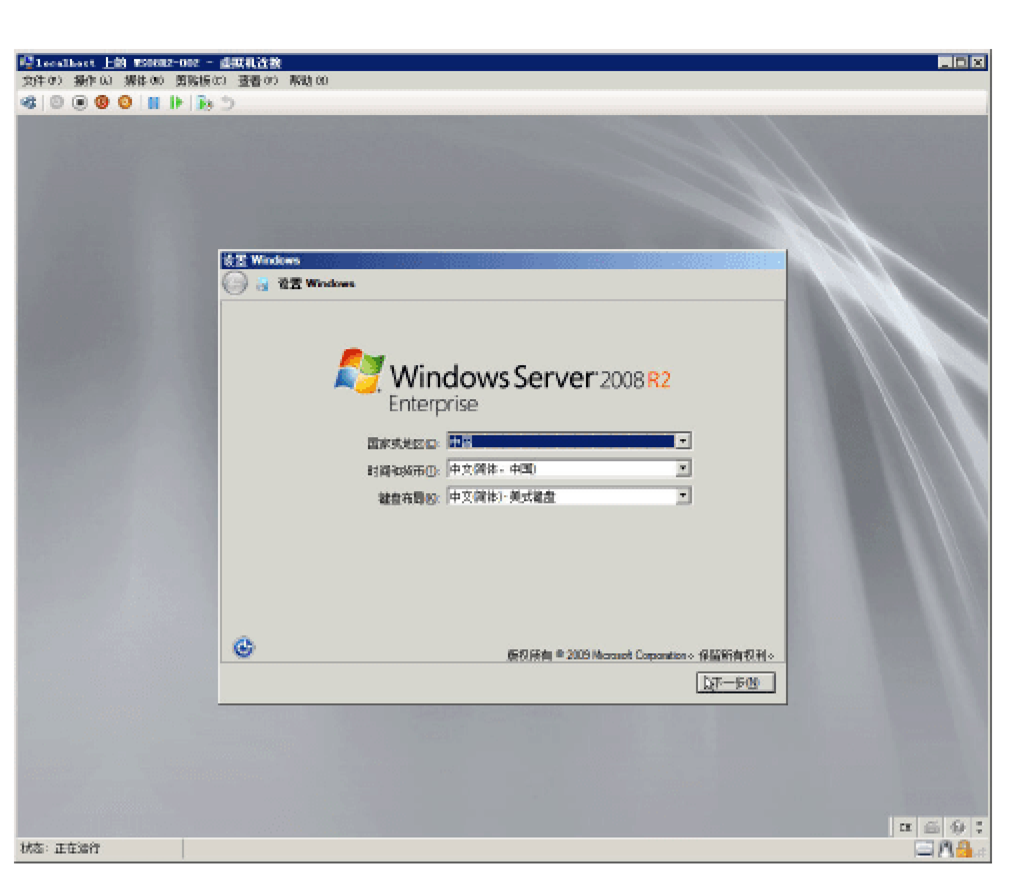


图 11-78　设置 Windows

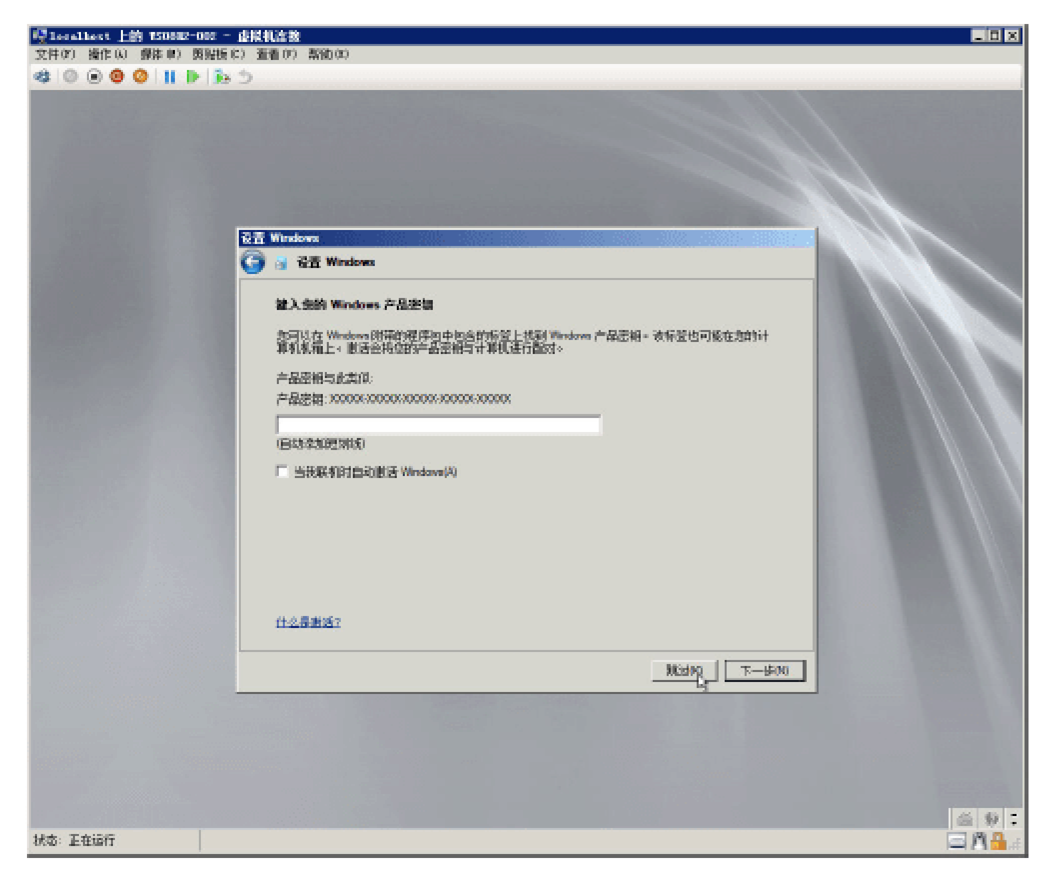


图 11-79　跳过产品密钥

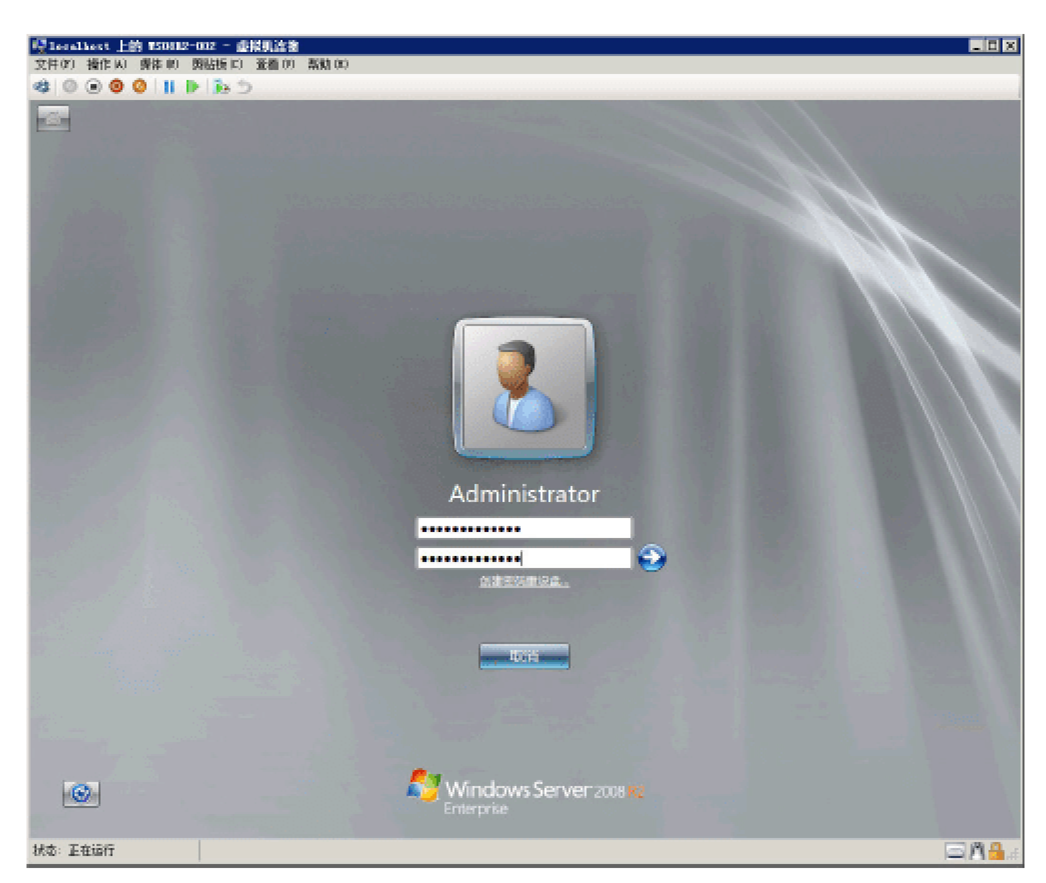


图 11-80　修改密码

05　进入系统，进行必要的设置后，关闭虚拟机，如图 11-81 所示。

06　关闭虚拟机之后，打开保存新虚拟机的虚拟磁盘文件夹，可以看到，新虚拟硬盘只占用了 365MB，如图 11-82 所示。这是在父磁盘的基础上，重新配置系统改动部分的大小。

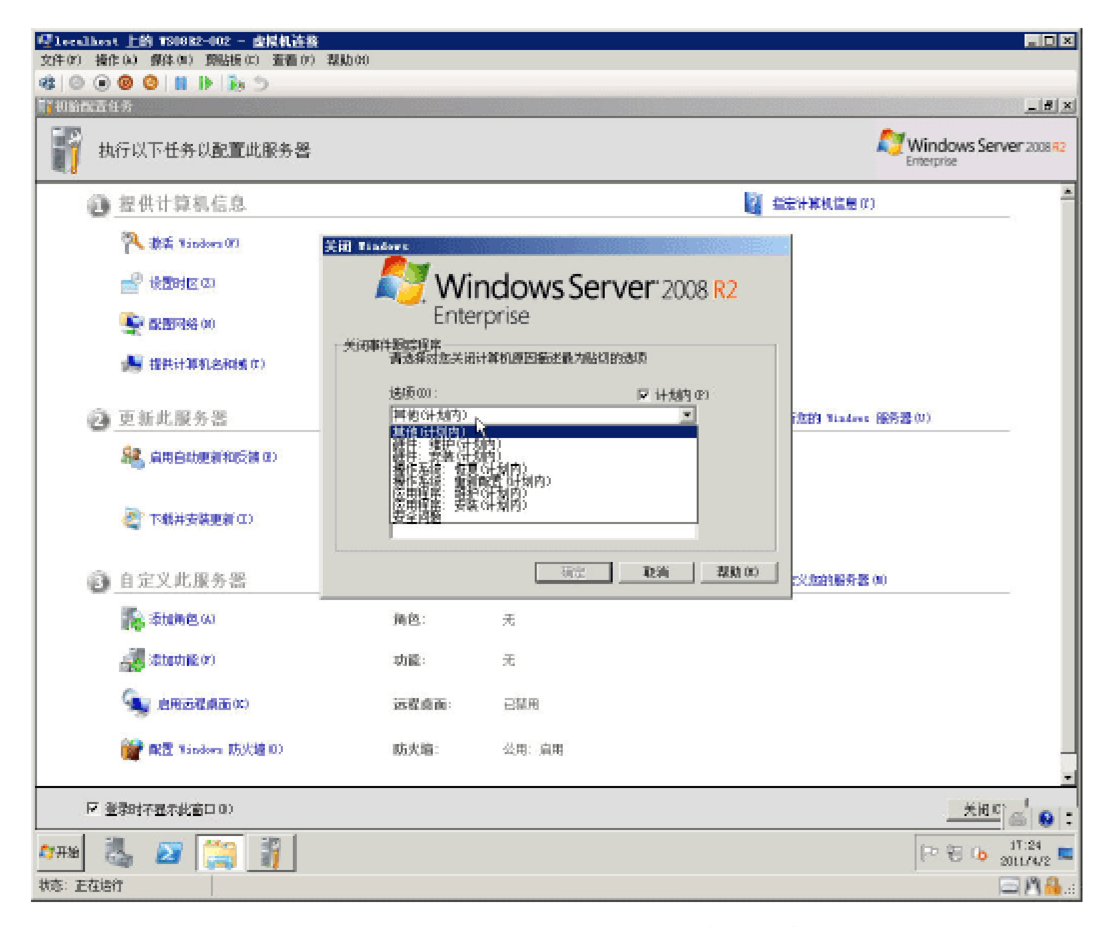


图 11-81　关闭虚拟机

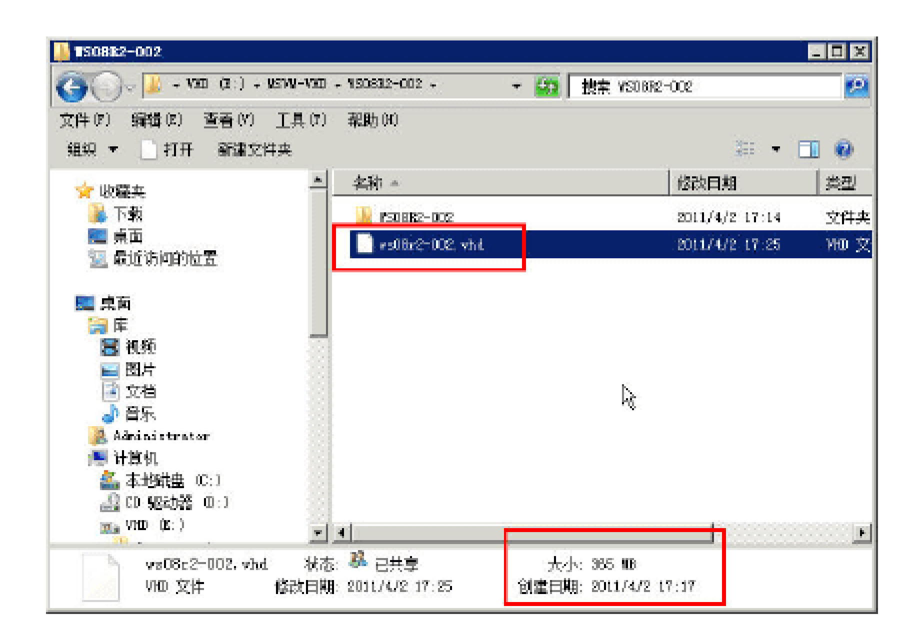


图 11-82　差异磁盘占用空间大小

07 打开虚拟机设置，在“硬盘驱动器”窗格中单击“检查”按钮，可以看到该虚拟机使用的是差异虚拟磁盘，以及虚拟硬盘的父磁盘属性及大小，如图 11-83 所示。

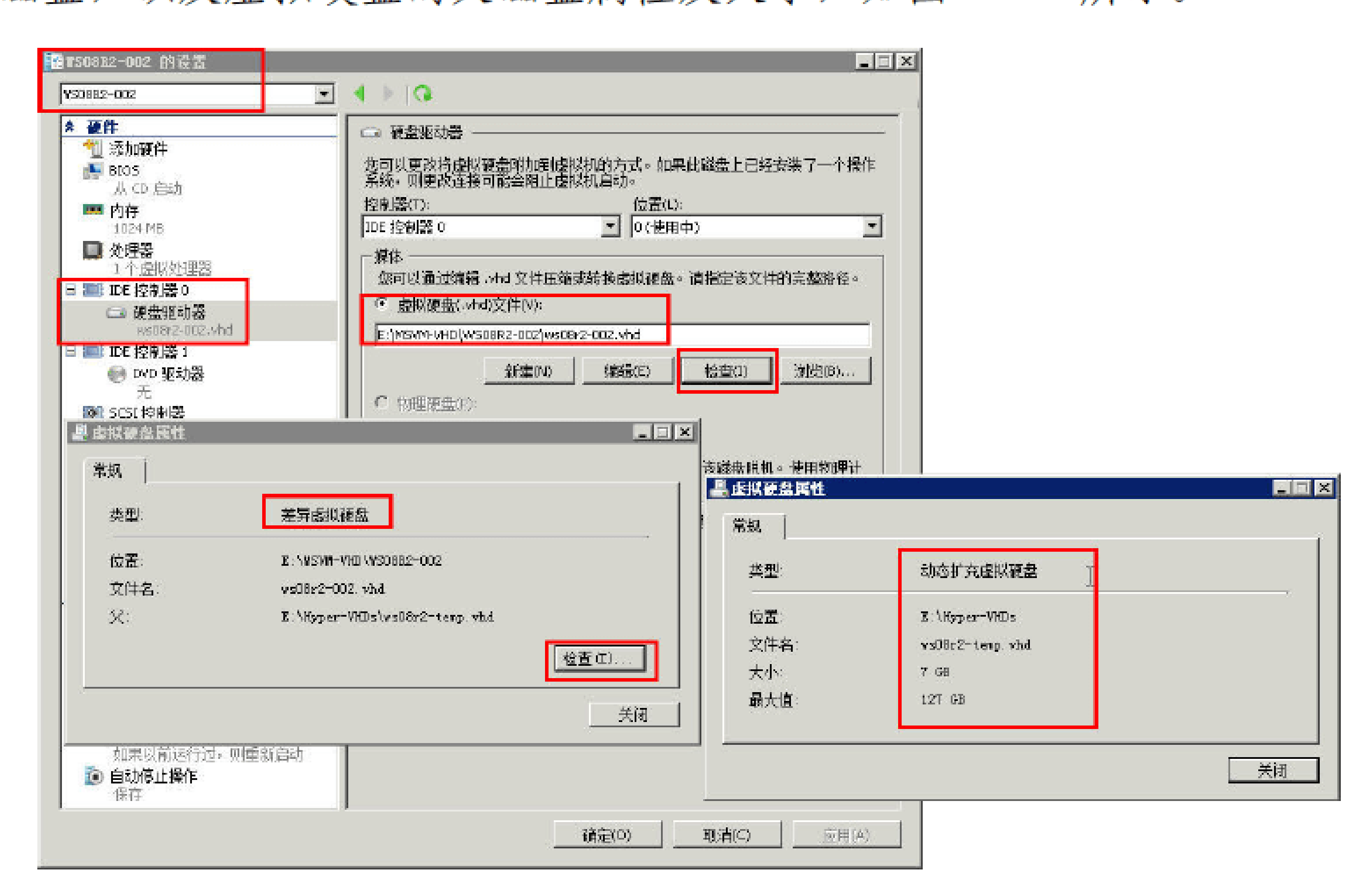


图 11-83　差异磁盘

第 12 章　使用 SCVMM 2008 R2 管理 Hyper-V

在本章，我们介绍 Microsoft 专用虚拟机管理工具 SCVMM 2008 R2 管理 Hyper-V 的内容。SCVMM 是 System Center Virtual Machine Management 的简称，目前最新版本是 2008 R2，修订补丁是 SP1。

接下来，我们将分以下几个内容进行介绍：

- 实验环境介绍。
- SCVMM 2008 安装部署。
- VMM 管理员安装与配置。
- 添加共享库服务器与库共享资源。
- 创建虚拟机、在虚拟机中安装操作系统。
- 虚拟机的模板的创建与使用。
- 虚拟机的迁移。

12.1　VMM 实验环境介绍

在本章的操作中，我们将在前面实验环境的基础上，在 Windows Server 2008 R2 With Hyper-V 的主机中，创建一个名为 scvmm 2008 R2 的虚拟机，在此虚拟机中安装 Windows Server 2008 R2、加入到域，安装 SCVMM 2008 R2，并管理 Hyper-V Server 与 Windows Server 2008 R2 With Hyper-V 这两个物理主机，实验拓扑如图 12-1 所示。在本章的实验中，会用到 dc.heinfo.local 与 datacenter.heinfo.local 两台服务器中的、保存各种安装镜像的共享文件夹。

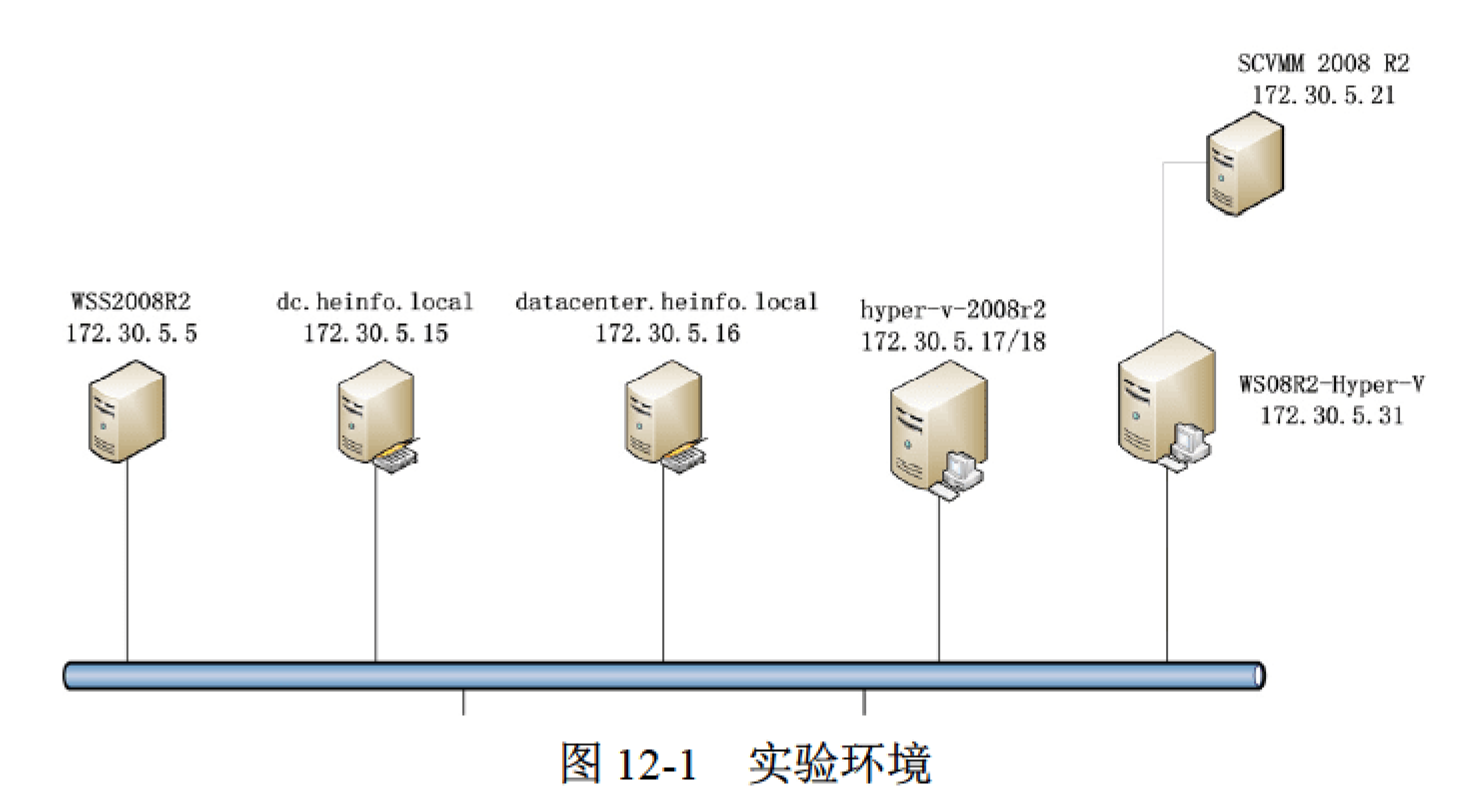


图 12-1　实验环境

使用 SCVMM 2008 R2 管理 Hyper-V 的网络拓扑如图 12-2 所示。

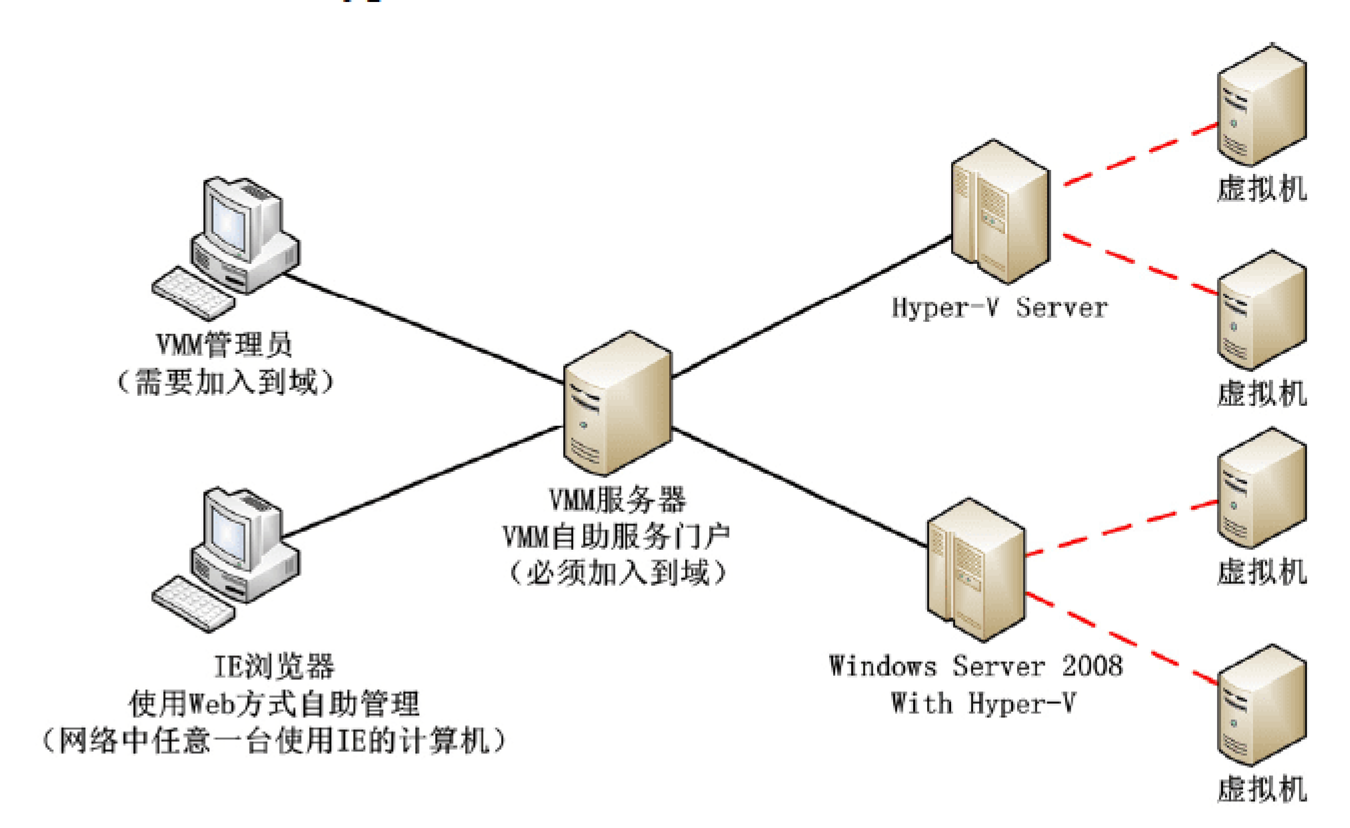


图 12-2　SCVMM 体系结构

在图 12-2 中，VMM 服务器是安装 System Center Virtual Machine Management 2008 R2 服务器的一台计算机，该计算机必须加入到域，并且使用域管理员账户登录，由这台服务器管理 Hyper-V Server 或安装有 Hyper-V 功能的 Windows Server 2008（以下简称"Hyper-V Server 主机"）。VMM 服务器是"客户/服务器"系统或"Browser/Server"系统，用户需要使用安装有"VMM 管理员"控制台的计算机，或者使用 IE 浏览器，登录安装并启用"VMM 自助服务门户网站"的"VMM 服务器"才能管理 Hyper-V Server 主机。

12.2　安装 SCVMM 2008 R2

使用上一节安装的 Windows Server 2008 R2，导出一台虚拟机，然后将导出目录重命名为 SCVMM 2008 R2，然后再将重命名后的虚拟机导入，导入之后，重命名虚拟机的名称为 scvmm2008r2，并修改虚拟机的配置，设置内存为 2GB、2 个虚拟处理器，然后安装 SCVMM 2008 R2，下面一一介绍。

12.2.1　准备 SCVMM 2008 R2 虚拟机

01 在 172.30.5.31 的物理主机中，使用"导出"、"导入"的方法，将以前安装好的一台 Windows Server 2008 R2 复制出一台虚拟机，并命名为 scvmm2008r2，设置虚拟机内存为 2048MB、2 个虚拟处理器，如图 12-3 所示。同时在"管理→自动启动操作"选择"始终自动启动此虚拟机"，这样该虚拟机将跟随主机一同启动。

02 然后启动该虚拟机，启动虚拟机后，重新设置计算机名称为 scvmm2008r2（当然也可以是其他的名称，这要看网络规划的情况），设置 IP 地址为 172.30.5.21/24、设置 DNS 地址为 172.30.5.15 与 172.30.5.16，如图 12-4 所示。

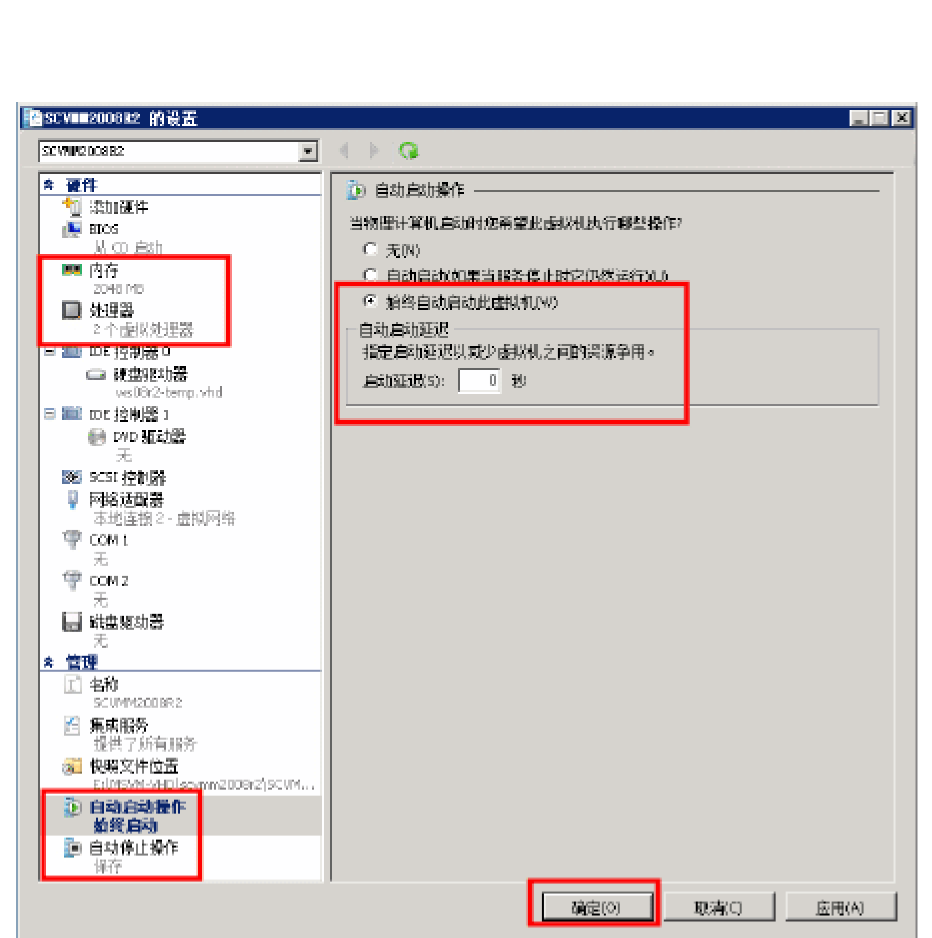


图 12-3　修改虚拟机的设置

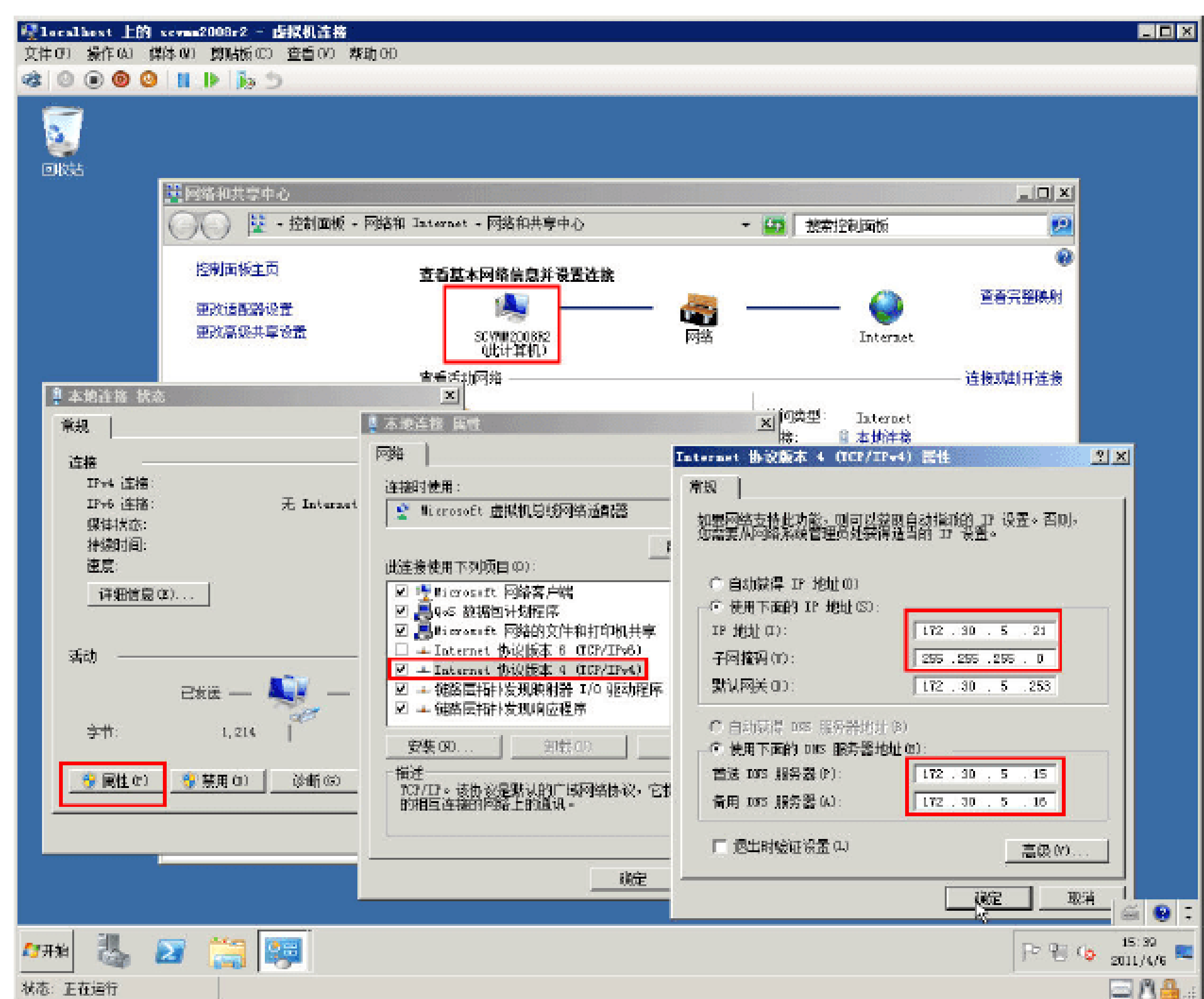


图 12-4　修改计算机名称、设置 IP 地址

然后将这台计算机加入到 heinfo.local，如图 12-5 所示。根据提示重新启动计算机。

03 再次进入系统之前，以域管理员账户登录，格式为 heinfo\administrator，同时输入域管理员账户密码，如图 12-6 所示。

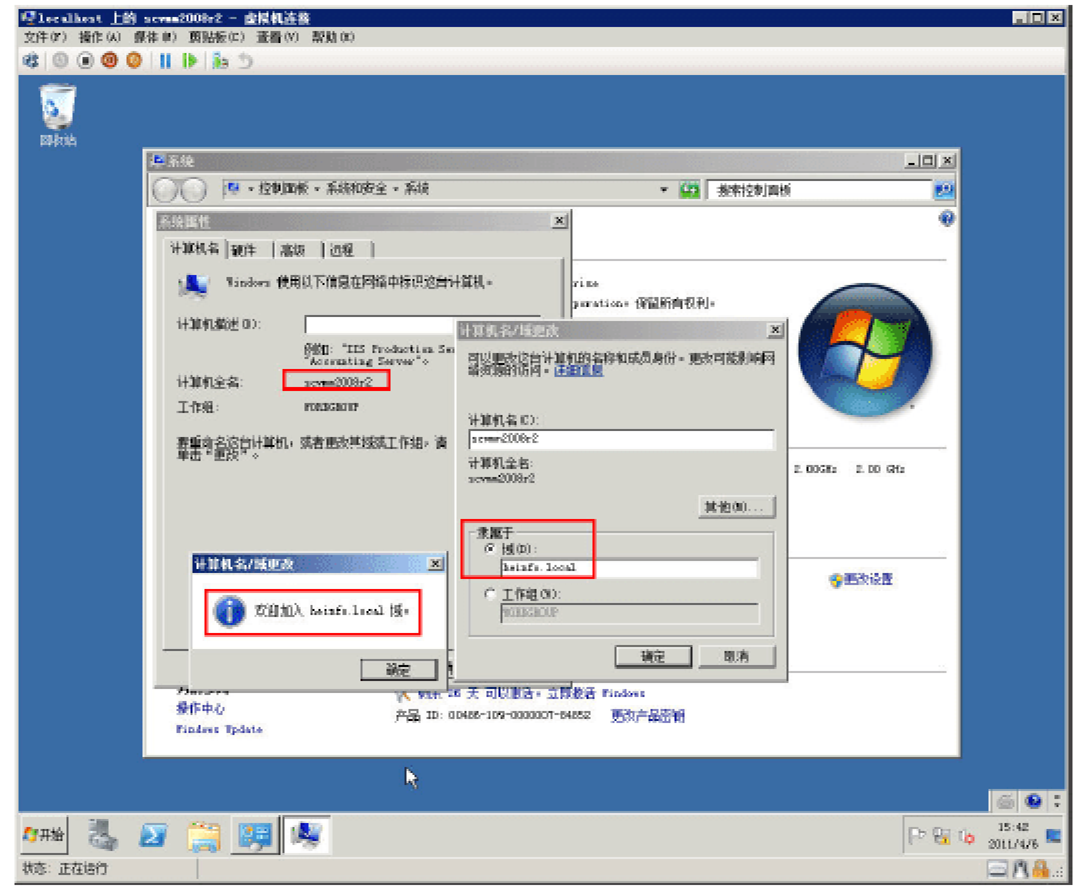


图 12-5　将计算机加入到域

图 12-6　以域管理员账户登录

12.2.2　安装 VMM 服务器

进入系统之后，选择"文件→设置"命令（如图 12-7 所示），进入虚拟机设置窗口，加载 SCVMM 2008 R2 With SP1 光盘镜像作为虚拟机的光驱，如图 12-8 所示。

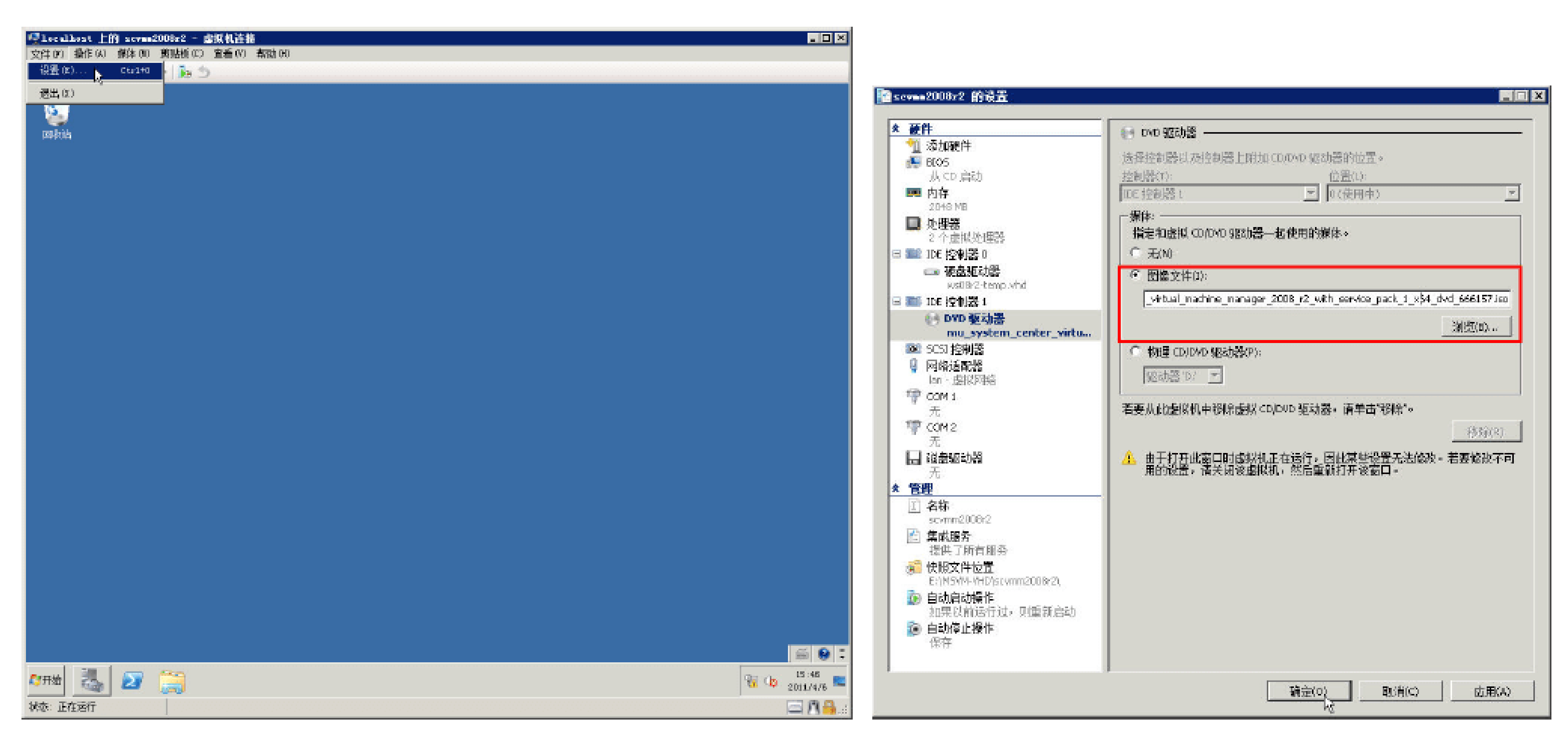


图 12-7　设置　　　　图 12-8　选择 SCVMM 安装光盘镜像作为虚拟机光驱

然后返回到虚拟机，开始安装 VMM 服务器，主要步骤如下。

01 在 SCVMM 2008 R2 安装界面中，单击“VMM 服务器”，如图 12-9 所示。

02 在“许可条款”对话框中，单击“我授受此协议的条款”单选按钮，如图 12-10 所示。



图 12-9　安装 VMM 服务器

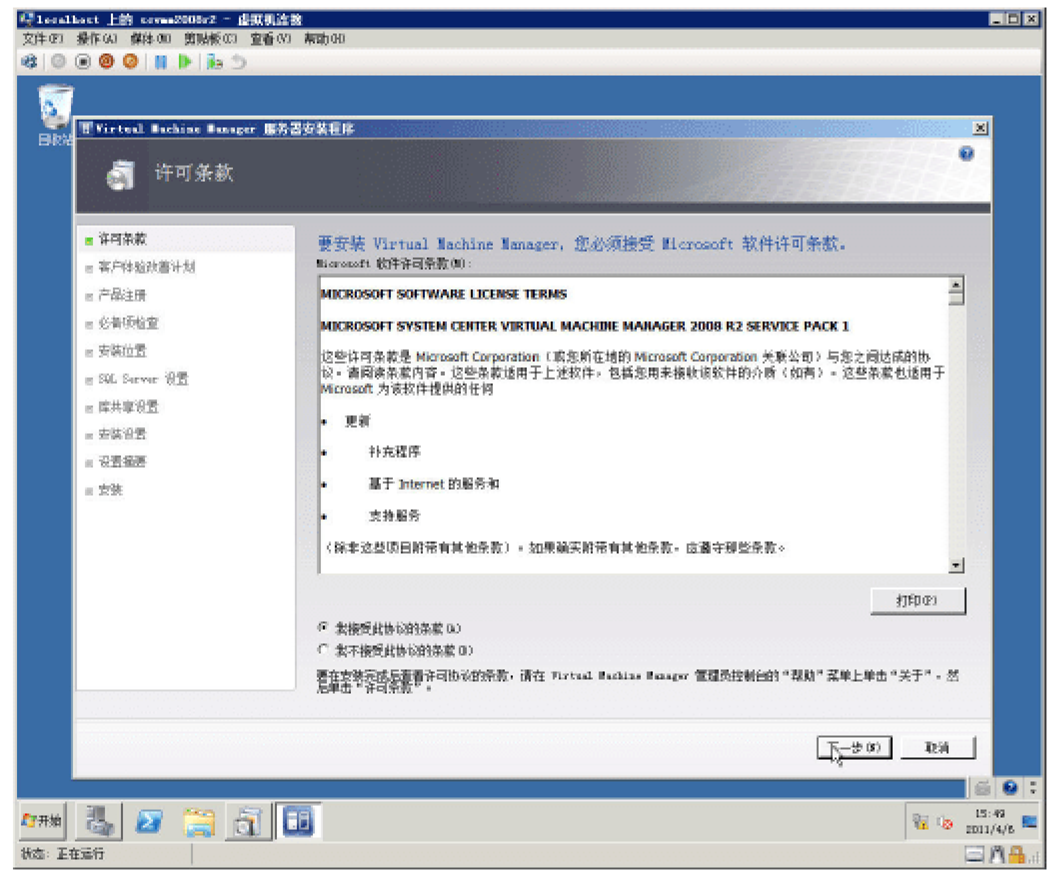


图 12-10　接受许可协议

03 在“必备项检查”对话框中，安装程序开始检查 SCVMM 2008 安装所必需的硬件与软件要求，只有检查通过之后才能安装，如图 12-11 所示。

04 在“SQL Server 设置”对话框中，选择“安装 SQL Server 2005 Express Edition SP3”，如图 12-12 所示。如果网络中有 SQL Server，也可以选择网络中的 SQL Server 作为 SCVMM 2008 的数据库。

05 在“安装设置”对话框中，选择通信端口与 VMM 服务器的服务账户，通常情况下保持默认值即可，如图 12-13 所示。

06 在“设置摘要”对话框中，复查 SCVMM 服务器的设置，检查无误之后，单击“安装”按钮开始安装，如图 12-14 所示。如果有任何问题，单击“上一步”按钮依次返回并修改。

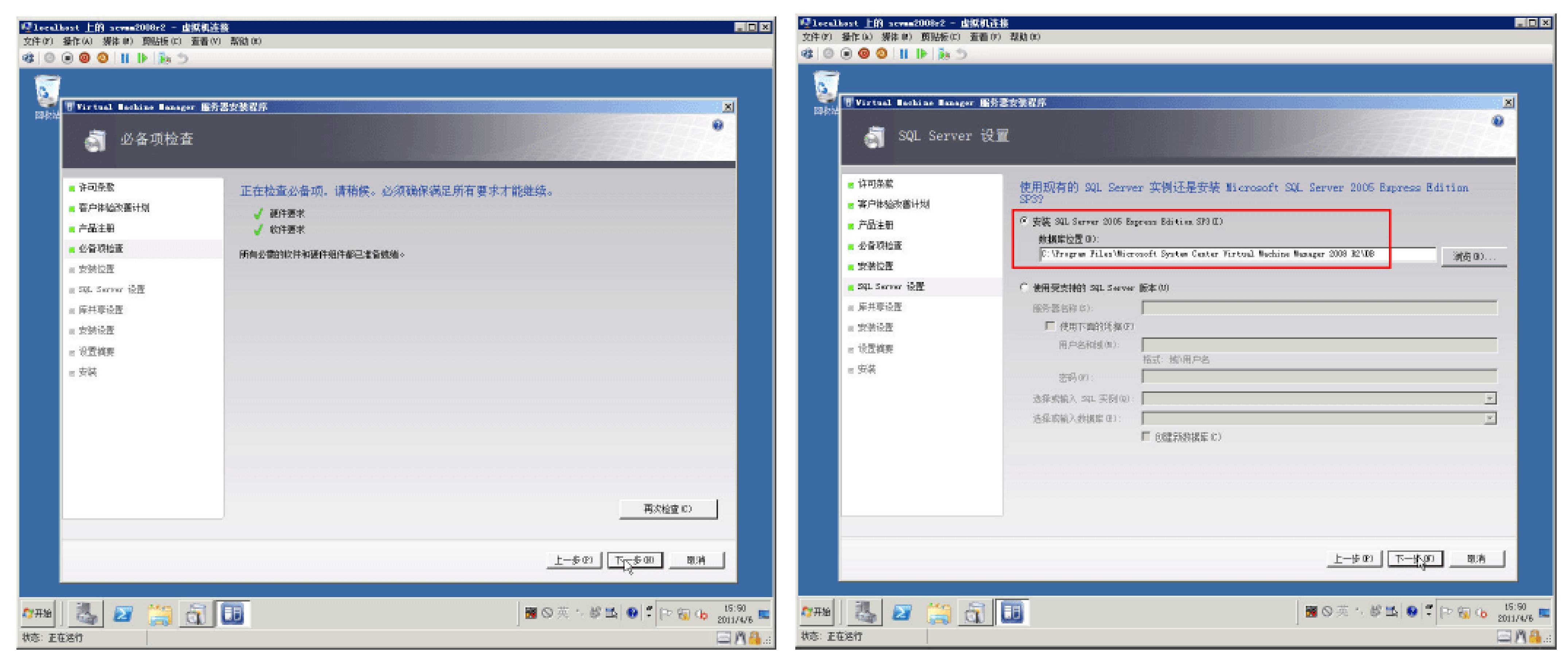


图 12-11　必备项检查　　　　图 12-12　安装 SQL Server 2005 Express 版本

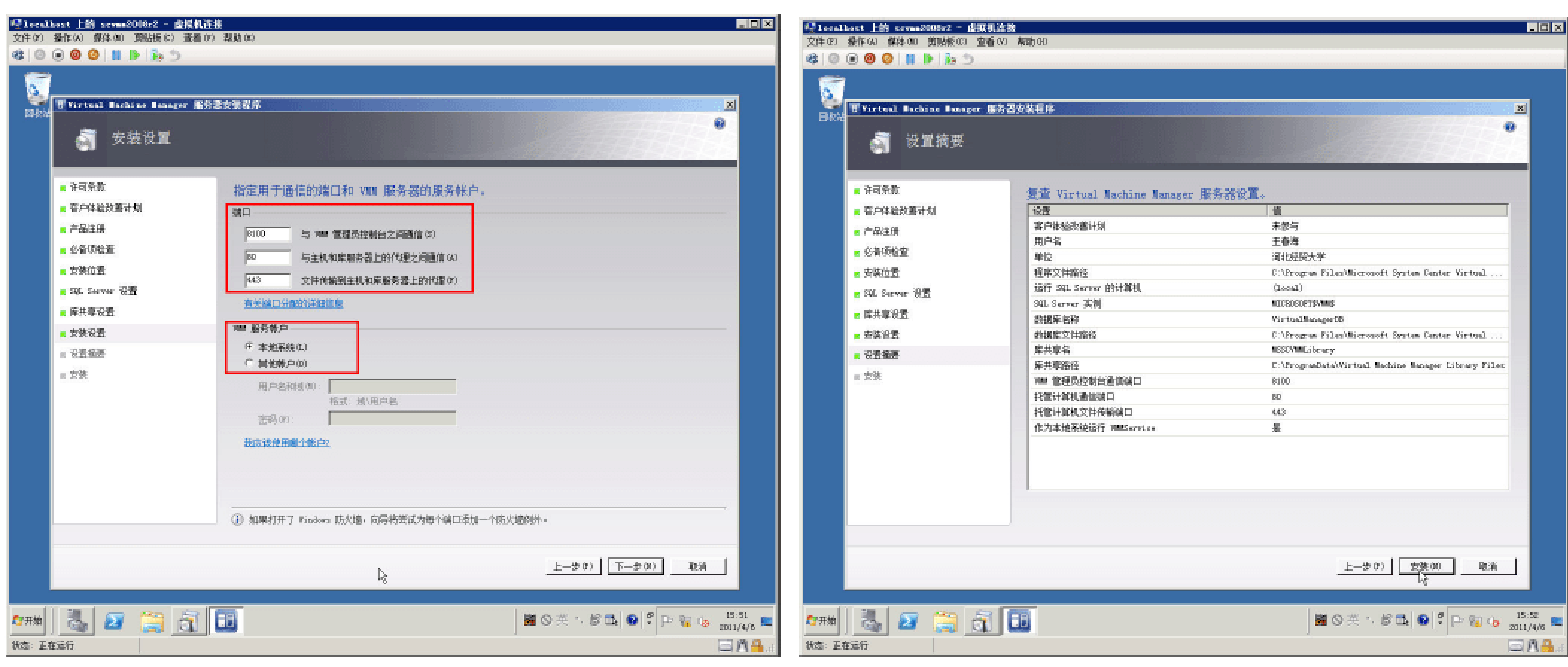


图 12-13　安装设置　　　　图 12-14　设置摘要

07 SCVMM 2008 R2 安装程序开始安装，大约 9min 左右，安装完成，单击“关闭”按钮，如图 12-15 所示。

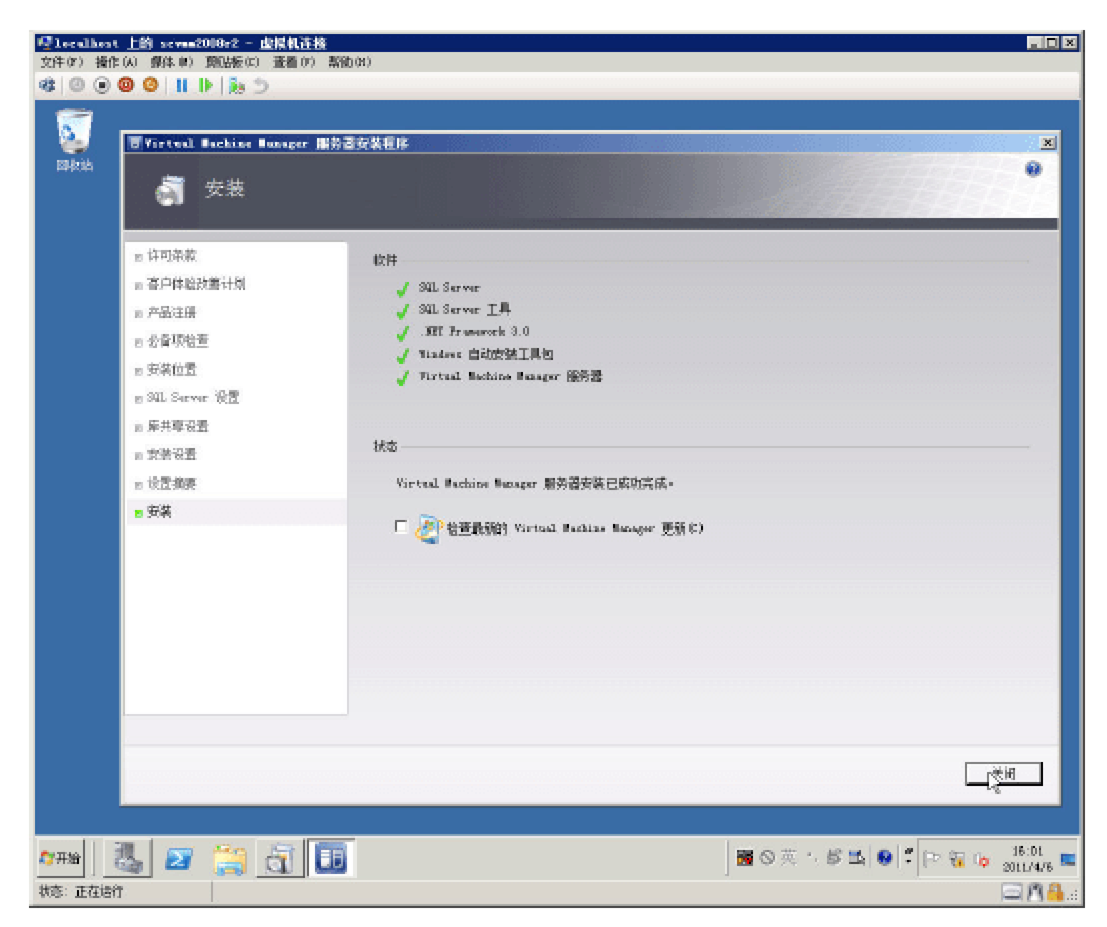


图 12-15　安装完成

如果只是单独做实验，可以将“VMM 管理员”程序也安装在“VMM 服务器”这台计算机上。但是，我们还是推荐，模拟真实的场景，在网络中的其他工作站上安装 VMM 管理员程序，然后再用 VMM 管理员程序连接到 VMM 服务器并管理 Hyper-V 计算机。接下来，我们介绍在网络中的其他工作站上安装 VMM 管理员程序的方法与配置步骤。

12.3　VMM 管理员安装与配置

“VMM 管理员”与“VMM 服务器”之间的关系，有点像 VMware 的 vSphere Client 与 VirtualCenter（新版本名为 vCenter Server）之间的关系，但又有所区别。vSphere Client 可以登录并连接到 VirtualCenter（或 vCenter Server）以管理 VMware ESX Server（或 VMware ESXi），也可以直接管理 VMware ESX Server（或 VMware ESXi）；而“VMM 管理员”目前的版本只能通过登录到“VMM 服务器”，并管理“VMM 服务器”以及通过“VMM 服务器”管理 Hyper-V Server 主机，还可以通过“VMM 服务器”连接到 VMware VirtualCenter 以管理 VMware ESX Server（或 VMware ESXi）。

12.3.1　在管理工作站上安装 VMM 管理员

把网络中的一台 Windows 7 计算机加入到 heinfo.local，运行 VMM 管理员程序，用这台计算机管理 VMM 服务器，并通过 VMM 服务器管理 Hyper-V Server 2008 虚拟化主机。首先介绍 VMM 管理员的安装过程，步骤如下。

01 把网络中的一台计算机加入到 heinfo.local，如图 12-16 所示。

02 加入到域之后，并以域管理员身份登录，然后运行 SCVMM 2008 R2 安装程序，在“安装程序”中单击“VMM 管理员控制台”，启动控制台安装，如图 12-17 所示。

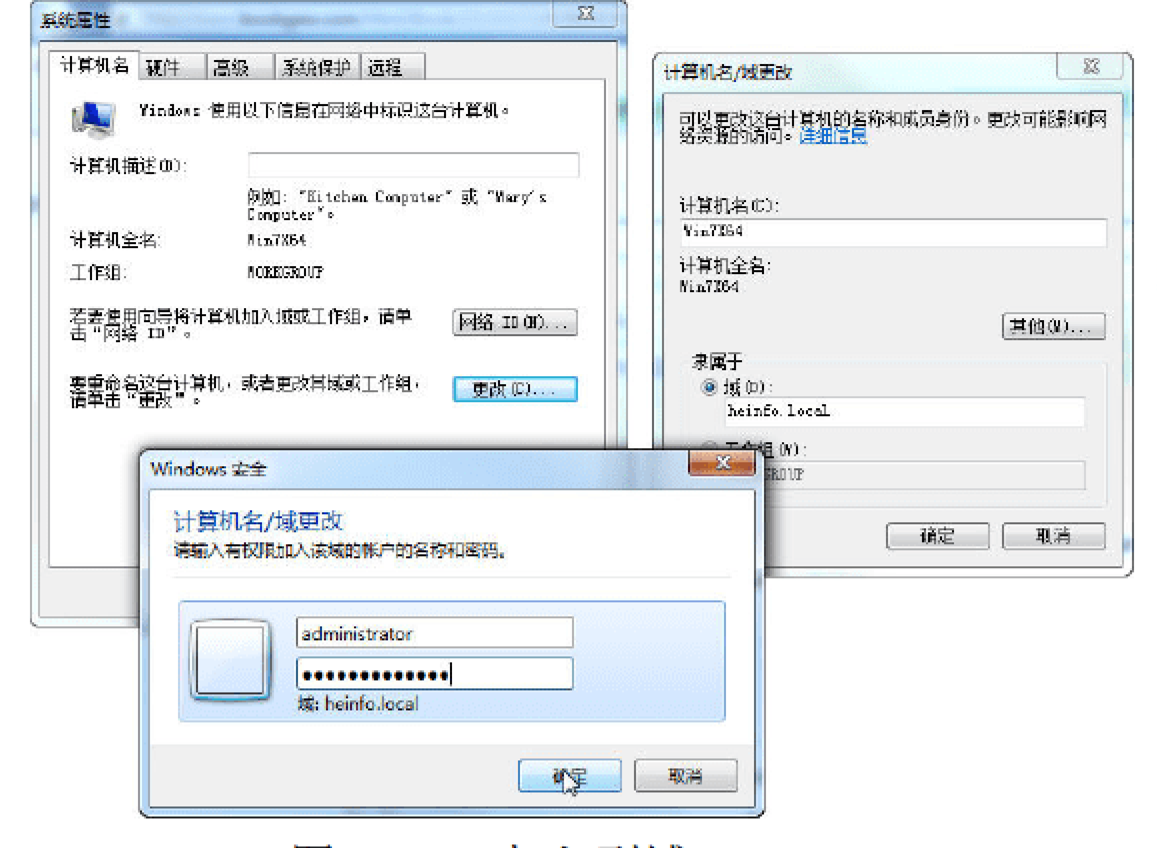


图 12-16　加入到域



图 12-17　VMM 管理员控制台

03 在“许可条款”对话框中，授受许可协议，如图 12-18 所示。

04 在“必备项检查”对话框中，检查通过之后才能继续安装，如图 12-19 所示。

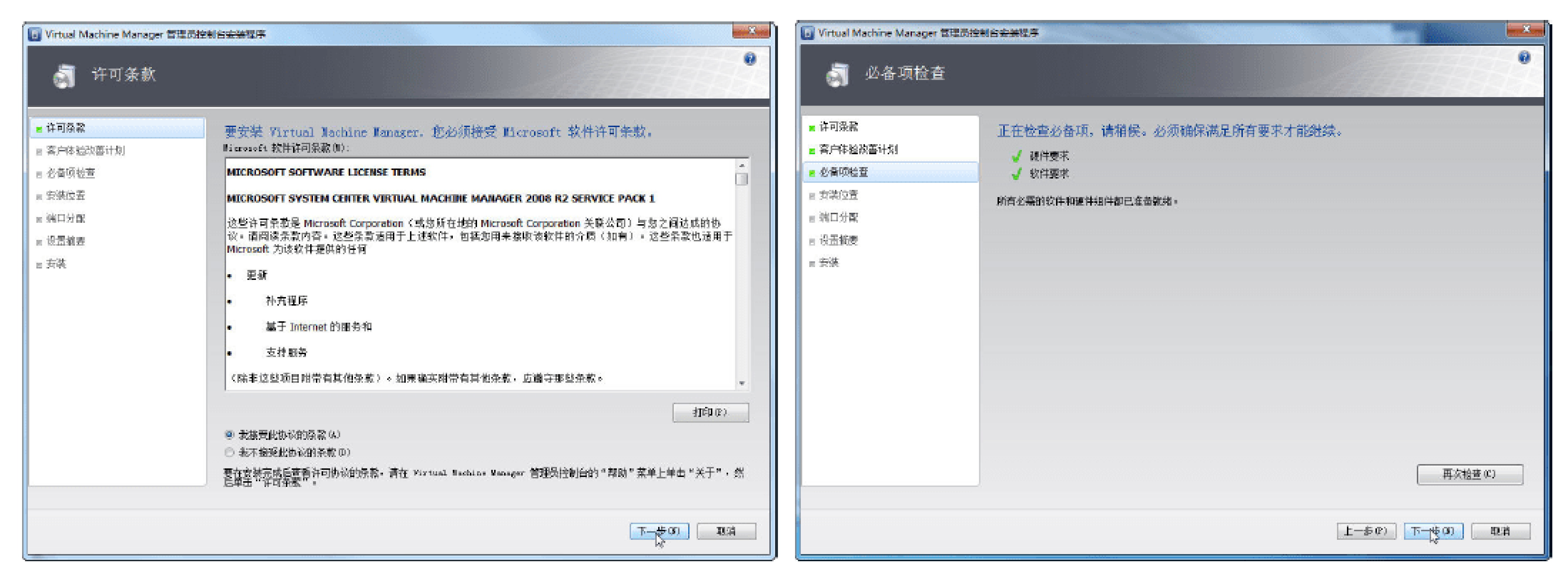


图 12-18　许可条款　　　　图 12-19　必备项安装

05 在“安装位置”对话框中，选择 VMM 管理员程序文件存储位置，如图 12-20 所示。

06 在“端口分配”对话框中，选择 VMM 管理员控制台与 VMM 服务器通信的端口，默认是 8100，如图 12-21 所示。

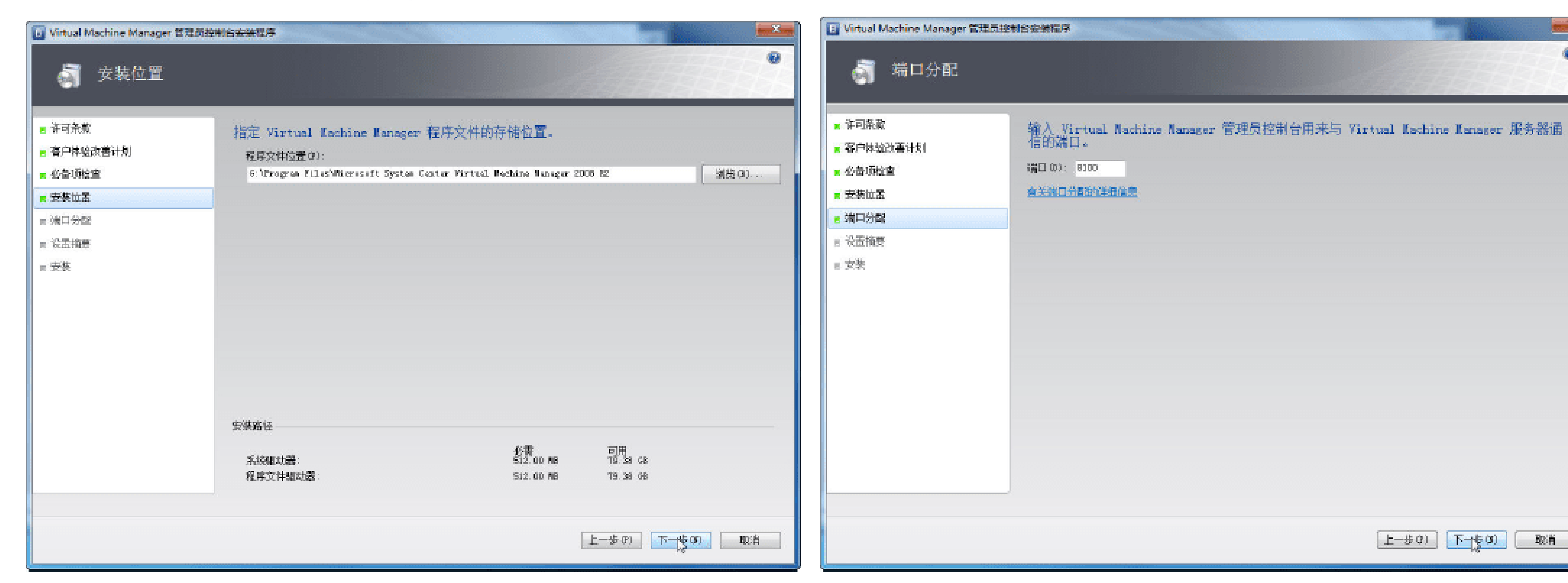


图 12-20　选择程序存储位置　　　　图 12-21　端口分配

07 在“设置摘要”对话框中，检查 VMM 管理员控制台设置，无误之后单击“安装”按钮，开始安装，如图 12-22 所示。

08 在安装完成之后，单击“关闭”按钮，如图 12-23 所示。

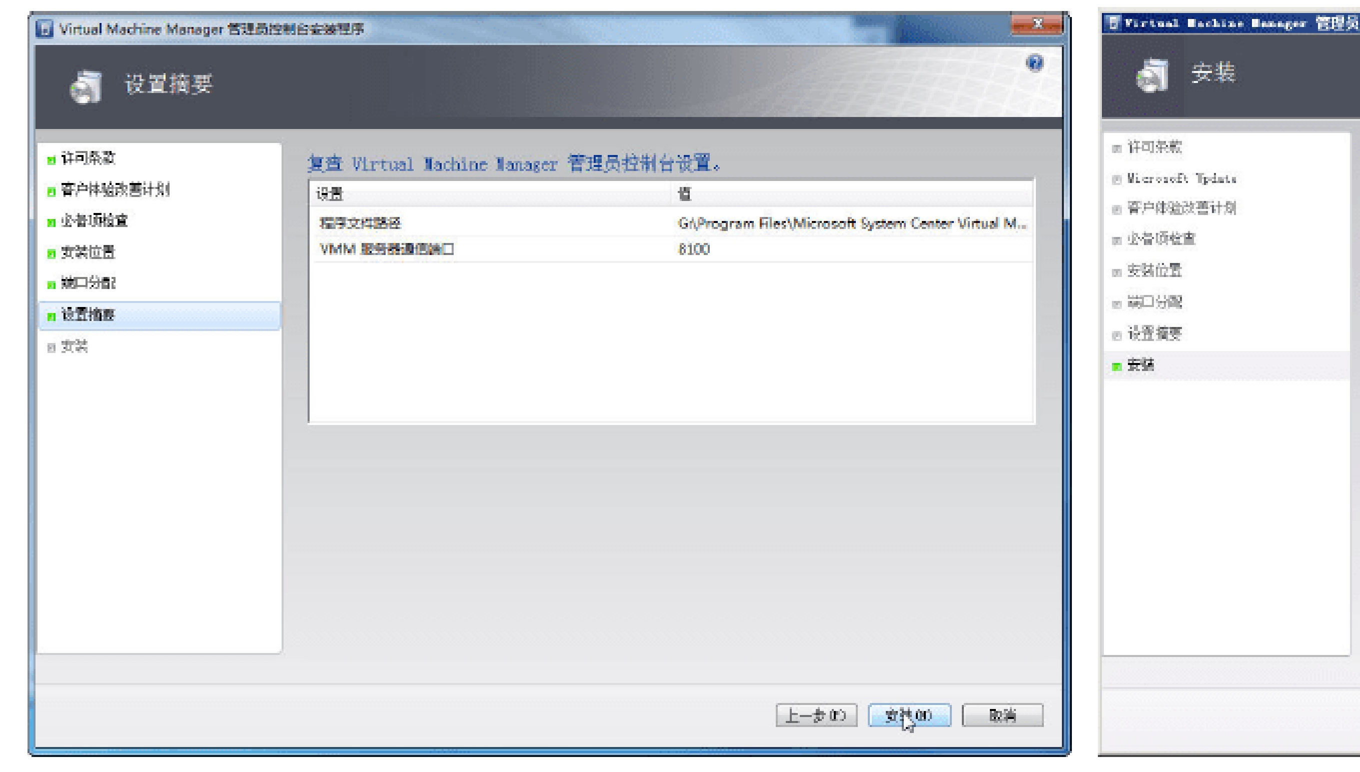


图 12-22 设置摘要

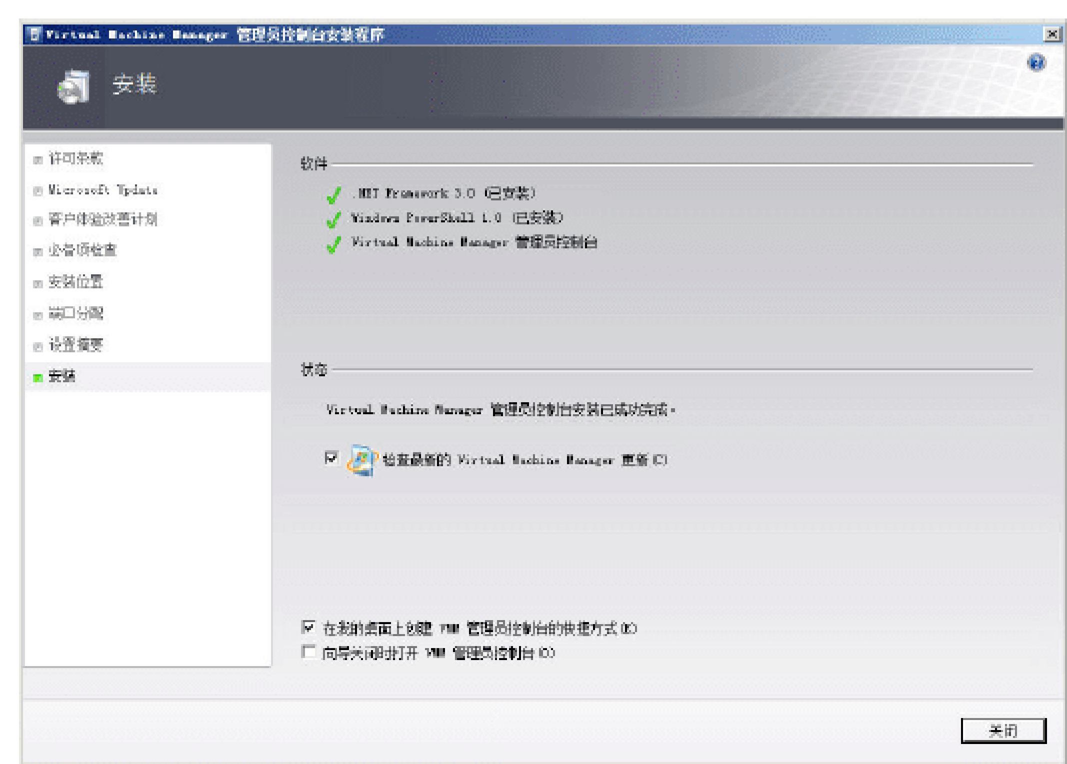


图 12-23　安装完成

09 在有的时候，会提示安装失败，如图 12-24 所示。

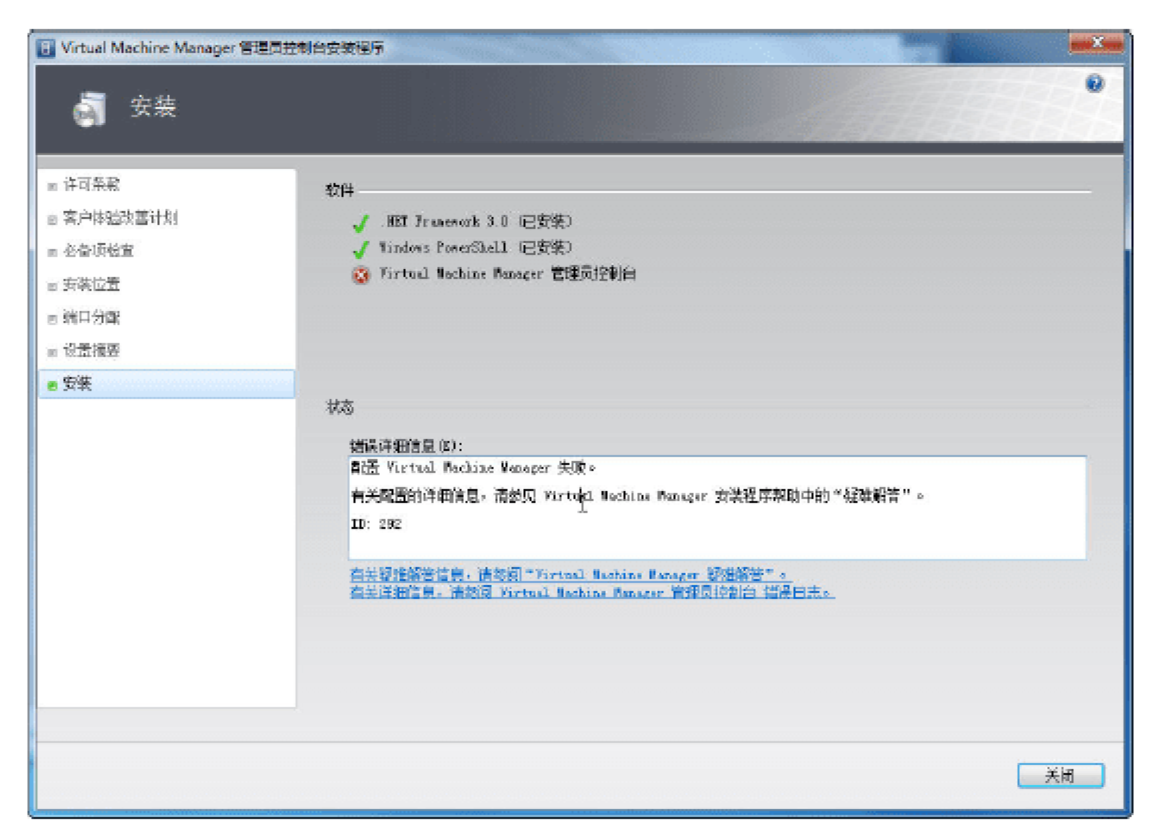


图 12-24　提示安装失败

但检查日志，发现安装成功，如图 12-25 所示。这种情况下，并不影响 VMM 管理员的使用。

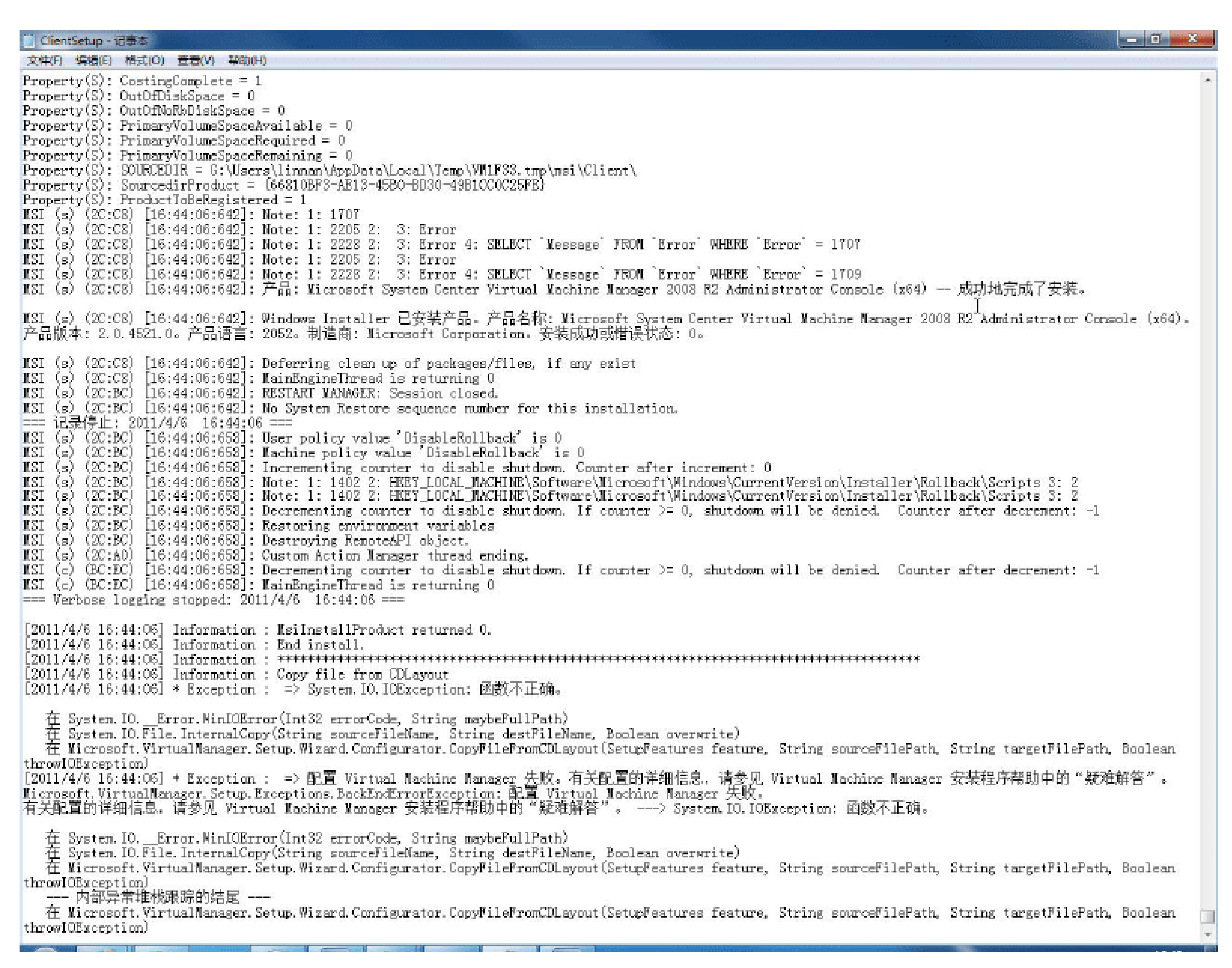


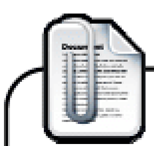
图 12-25　安装完成但配置失败

12.3.2　使用 VMM 管理员控制台添加虚拟化主机

在安装好 VMM 管理员控制台之后，登录 VMM 服务器并添加虚拟化主机，首先创建一个主机组，步骤如下。

01 在“连接到服务器”对话框中，输入 VMM 服务器的 IP 地址或计算机名称。在本例中是 vmm.heinfo.local，端口是 8100，并选中“将此服务器设置为我的默认服务器”复选框，如图 12-26

所示。



说 明

需要在域控制器中，添加名为 VMM 的 A 记录，该记录指向“VMM 服务器”的 IP 地址，本例中是 172.30.5.21。如果没有创建该 A 记录，可以输入 VMM 服务器的 IP 地址或 DNS 名称。

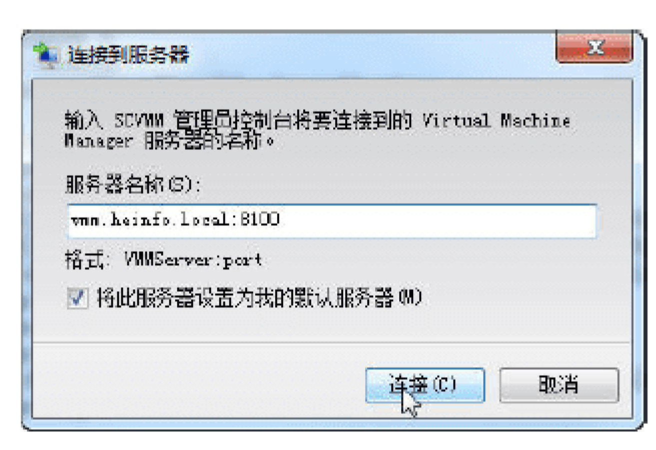


图 12-26 连接到服务器

02 连接到服务器之后，登录到 VMM 服务器，右击“所有主机”，选择“新建主机组”，如图 12-27 所示。

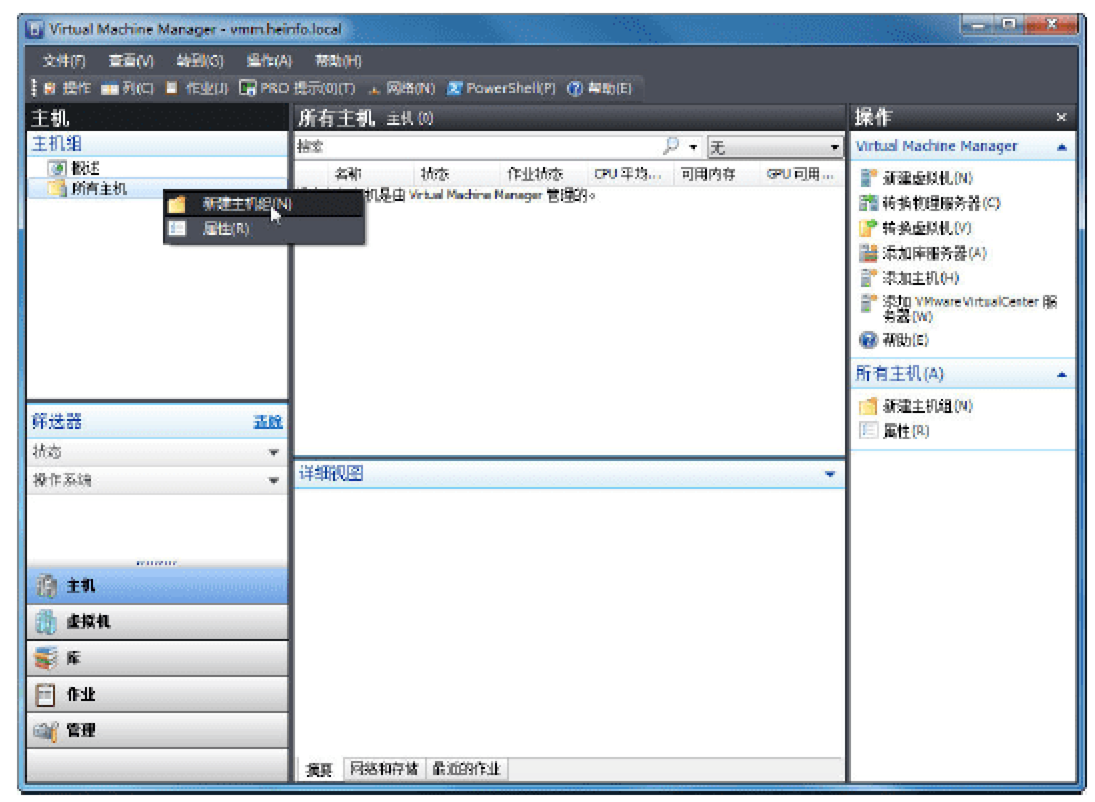


图 12-27 新建主机组

03 在本例中，设置主机组名为“Hyper-V”。

在添加“主机组”后，就可以向主机组中添加虚拟化主机了，可以添加启用了 Hyper-V 功能的 Windows Server 2008、Windows Server 2008 R2，或者 Hyper-V Server 2008、Hyper-V Server 2008 R2，或者 Microsoft Virtual Server 2005。在本例中，我们将添加本次实验的 2 台主机，并且这 2 台主机都已经加入到了 Active Directory，步骤如下。

01 在 VMM 管理员控制台左侧任务窗格中选中主机组，在右侧任务窗格中单击“添加主机”链接，如图 12-28 所示，进入添加主机向导。

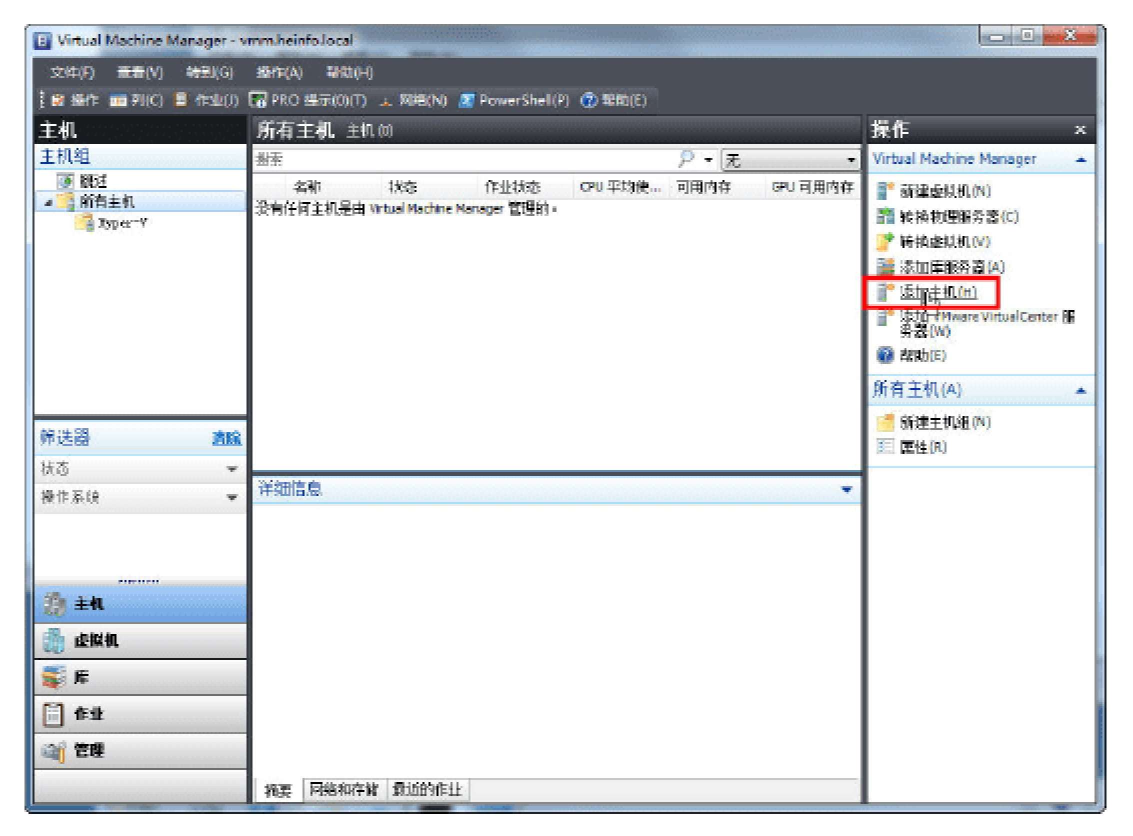


图 12-28 添加主机

02 在“选择主机位置”对话框中，在“选择主机位置，然后输入必需的凭据”处，选择要添加的主机的位置。在本例中，所有的（虚拟化）主机都已经添加到 Active Directory，所以选中“位于 Active Directory 域中的基于 Windows Server 的主机”单选按钮，在“输入凭据连接到主机”处，输入域管理员账户与密码，并且输入域名，同时选中“主机处于受信任的域中”复选框，如图 12-29 所示。

03 在“选择主机服务器”对话框中，单击“搜索”按钮，用来搜索网络中的主机，如图 12-30 所示。

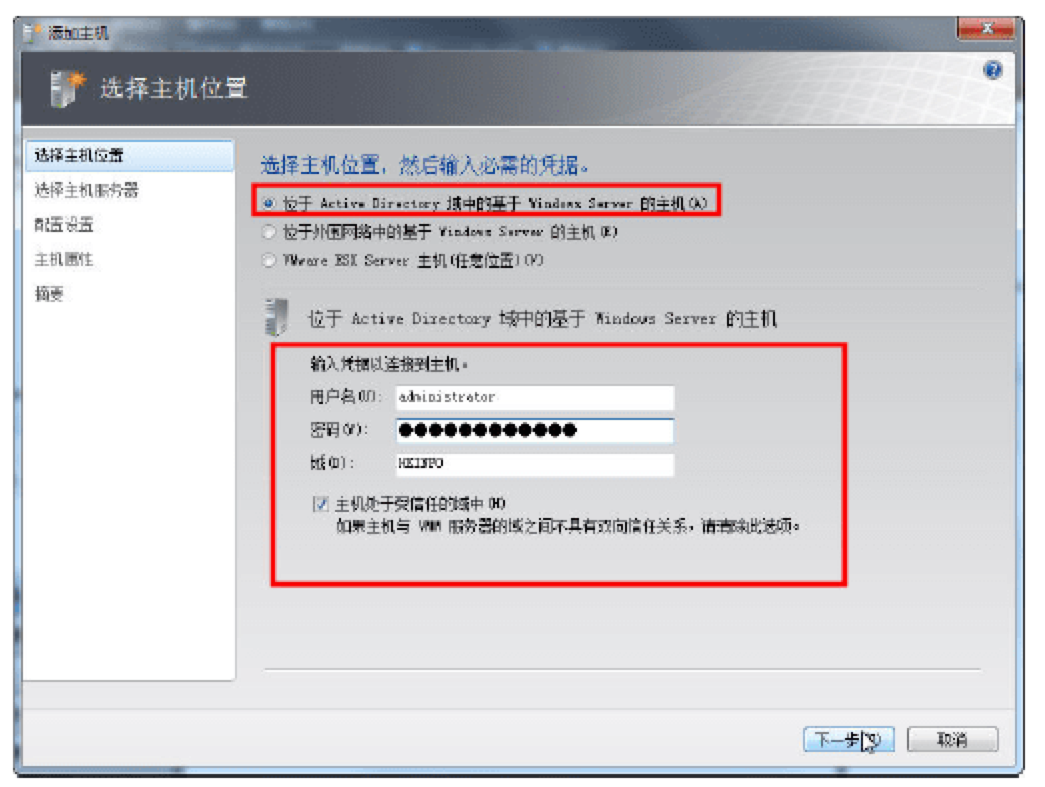


图 12-29　选择主机位置与管理员凭据

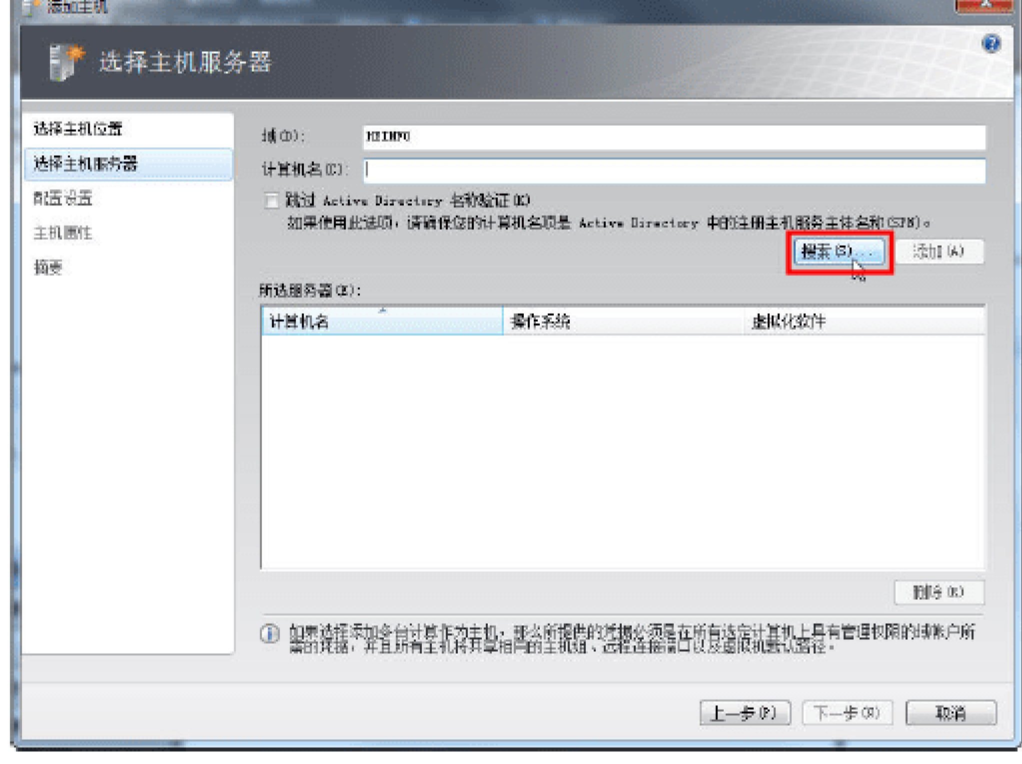


图 12-30　搜索

04 在“计算机搜索”对话框中，在“搜索条件”处选中“Hyper-V”复选框，然后单击“搜索”按钮，这样会把当前 Active Directory 域中所有具有 Hyper-V 功能的主机搜索并显示出来，而不显示其他的主机。在本例中，会搜索出 2 台 Hyper-V 主机，一台是 Windows Server 2008 R2，并启用了 Hyper-V 功能，另一台则是 Hyper-V Server 主机，选中之后，单击“添加”按钮，然后单击“确定”按钮，如图 12-31 所示。

05 如果不对搜索过程进行过滤，则会搜索出当前 Active Directory 中所有的主机，如图 12-32 所示。在这种情况下，可以单击“虚拟化软件”进行排序，同样可以选中所需要的主机。



图 12-31　搜索主机并进行过滤

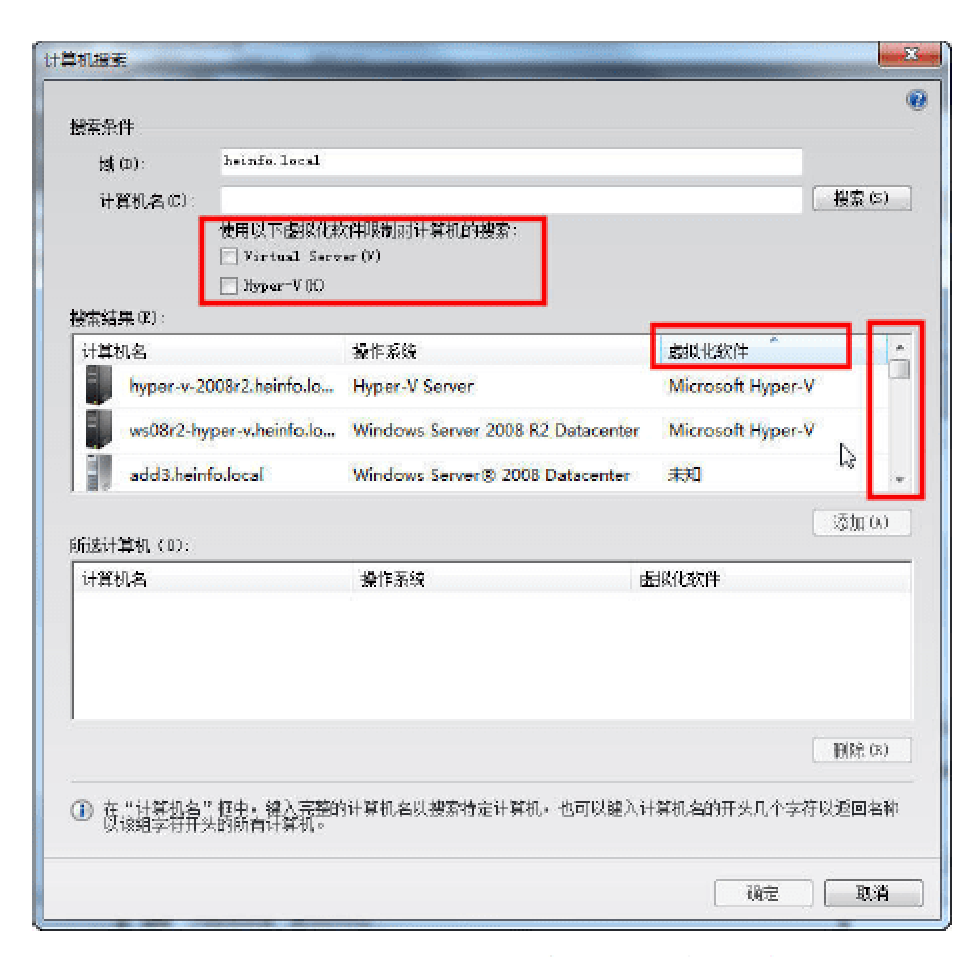


图 12-32　搜索出所有主机

06 选中主机之后，返回到“选择主机服务器”对话框，在此会列出上一步所选择并添加的虚拟化主机，如图 12-33 所示。

07 接下来会出现一个警告对话框，提示当前添加的一台或多台主机运行的是 Windows Server 2008 操作系统或者更高版本，如果这些版本没有安装 Hyper-V 功能，VMM 在执行添加主机的过程期间，会自动启用这些角色并会导致服务器重新启动。单击“是”按钮继续，如图 12-34 所示。

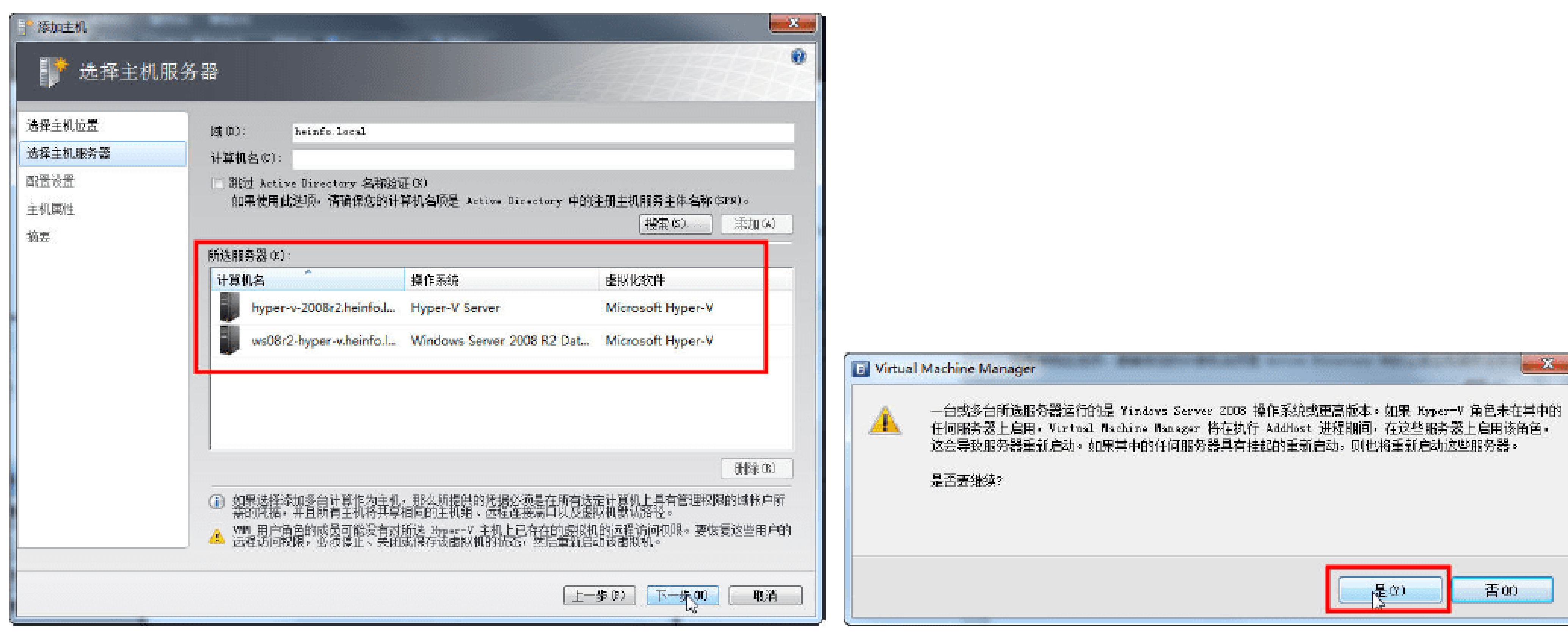


图 12-33　选择主机服务器　　图 12-34　警告信息

08 在“配置设置”对话框中，选择将所选的主机要添加到的主机组，如图 12-35 所示。在此，选择前面创建的名为“Hyper-V”的主机组。

09 在“主机属性”对话框中，选择添加虚拟机路径或使用默认路径，由于添加了多个主机，将在以后单独进行配置，单击“下一步”按钮，如图 12-36 所示。

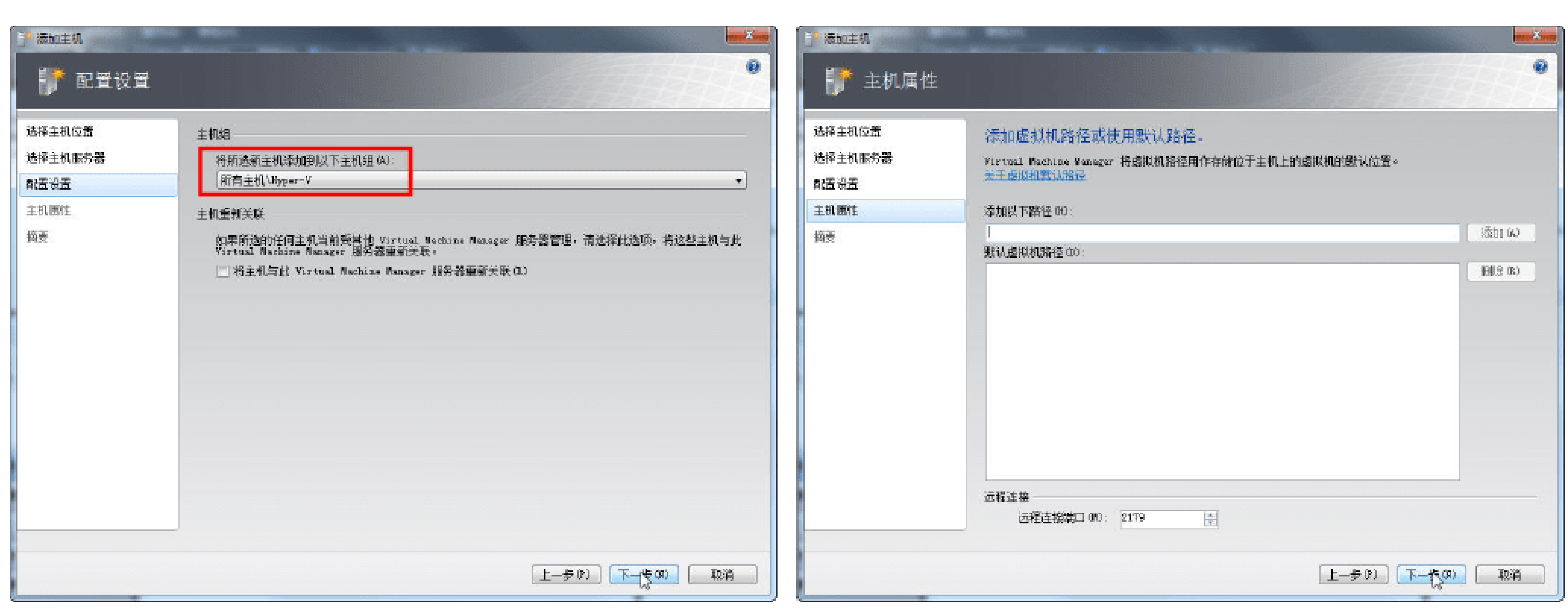


图 12-35　配置设置　　图 12-36　主机属性

10 在“摘要”对话框中，显示当前的操作，检查无误之后，单击“添加主机”按钮，如图 12-37 所示。如果有任何问题，单击“上一步”按钮返回进行检查。

11 然后弹出“作业”对话框，开始添加虚拟主机，如图 12-38 所示，直到添加主机完成。

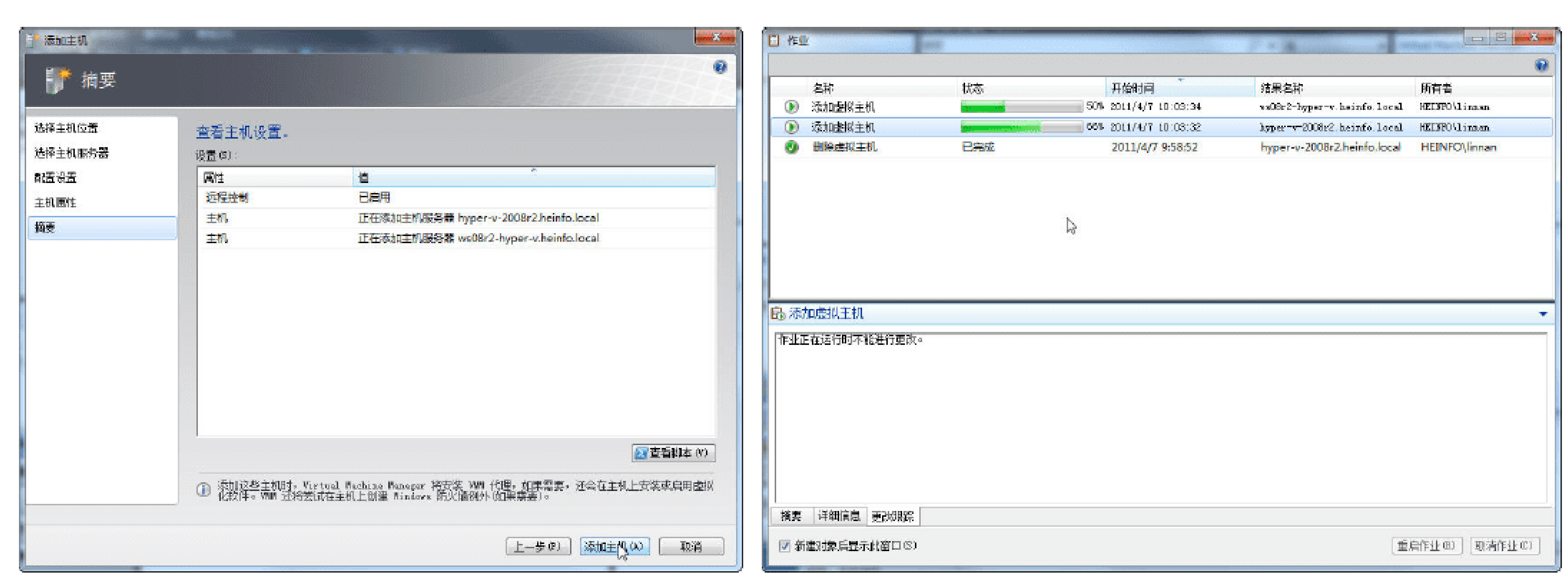


图 12-37 摘要　　　　图 12-38 作业

12 添加主机完成之后，返回到 VMM 管理员控制台，在“所有主机”列表中，显示了添加的虚拟化主机的名称、状态、作业状态、CPU、内存等消息，如图 12-39 所示。

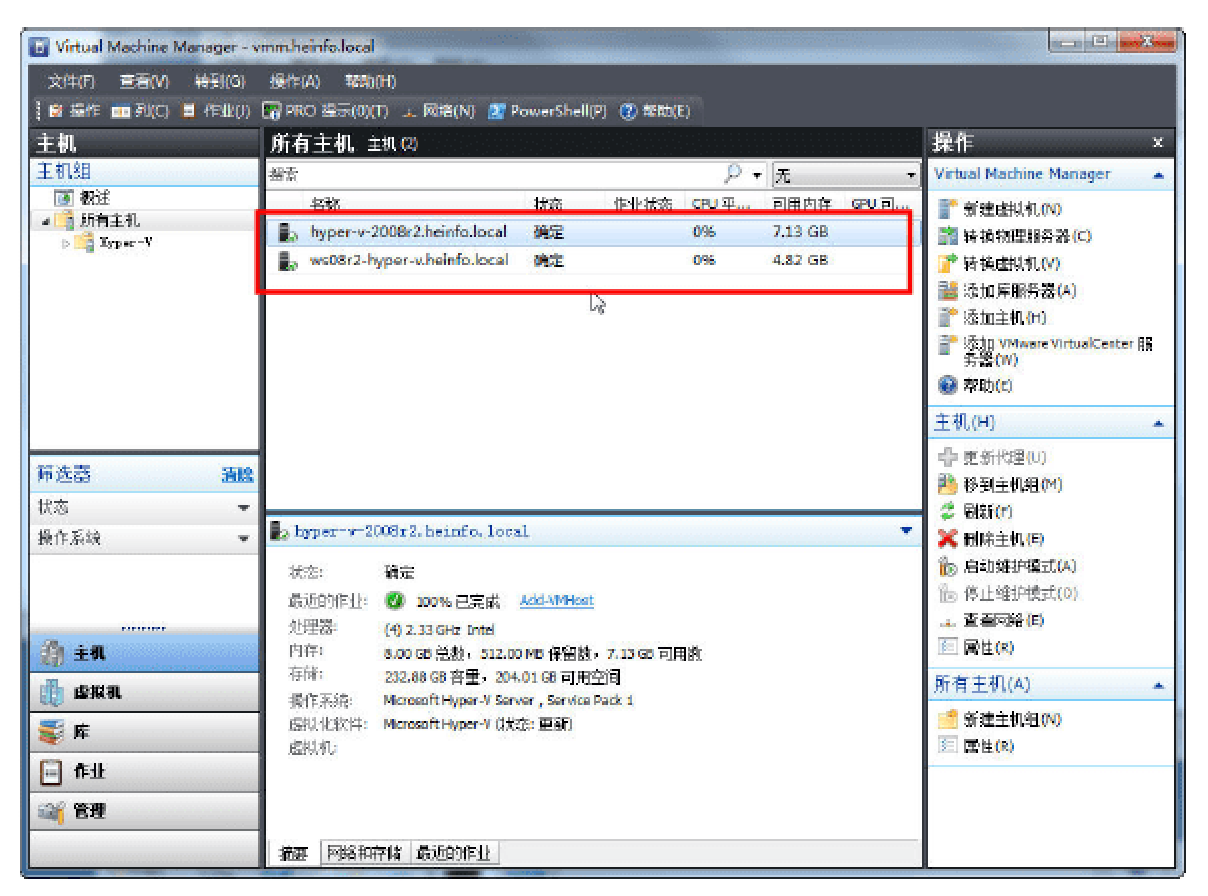


图 12-39 添加主机完成

12.3.3 添加（操作系统镜像文件的）共享资源库

在使用 Hyper-V 管理器管理 Hyper-V Server 时，要创建虚拟机并在虚拟机中安装操作系统，可以直接使用 Hyper-V 主机上的镜像文件。而在使用 VMM 服务器，创建虚拟机并在虚拟机中安装操作系统时，并不能以“本地”文件的方式使用保存在 Hyper-V 主机中的镜像文件，而是以“共享文件夹”的方式访问，并且需要将“共享文件夹”添加到 VMM 服务器的“库”中进行统一管理。

在本次的实验中，网络中的 2 台域控制器中保存了所有的 Microsoft 的操作系统的光盘镜像，并且在 Windows Server 2008 Hyper-V 主机中，也有一部分操作系统镜像文件。在下面的操作中，我们把这 3 台服务器中的镜像文件所在的“共享文件夹”，添加到 VMM 库服务器中进行统一管理。

01 在 VMM 管理员控制台中，单击右侧的“添加库服务器”链接，如图 12-40 所示。

02 在“输入凭据”对话框中，输入域管理员账户（或者具有域管理员功能的账户），如图 12-41 所示。

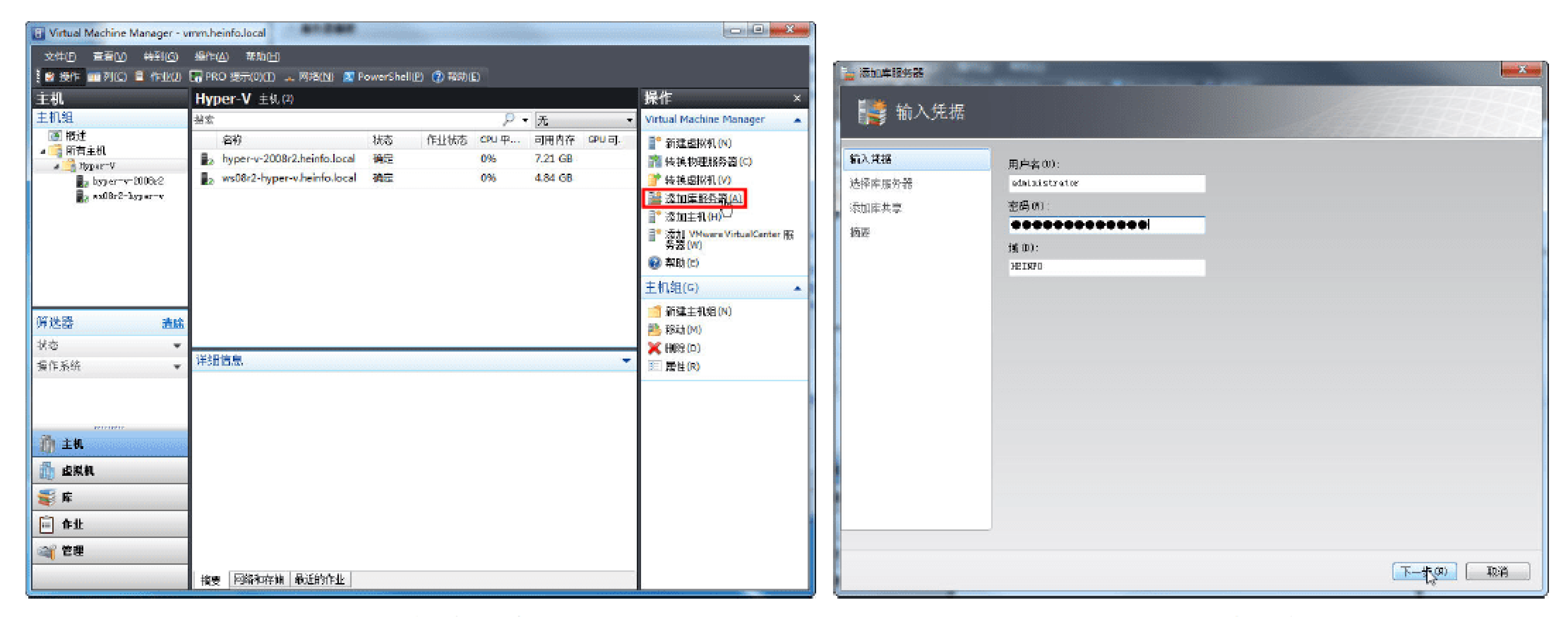


图 12-40 添加库服务器　　　　图 12-41 输入凭据

03 在“选择库服务器”对话框中，单击“搜索”按钮，如图 12-42 所示。

04 在“计算机搜索”对话框中，单击“搜索”按钮（不要选中 Hyper-V），并在“搜索结果”列表中，选择 2 台域控制器主机以及安装有 Hyper-V 功能的 Windows Server 2008 R2，然后将其添加到“所选计算机”列表中，这 3 台计算机中保存了 Windows 操作系统的安装光盘镜像，如图 12-43 所示。

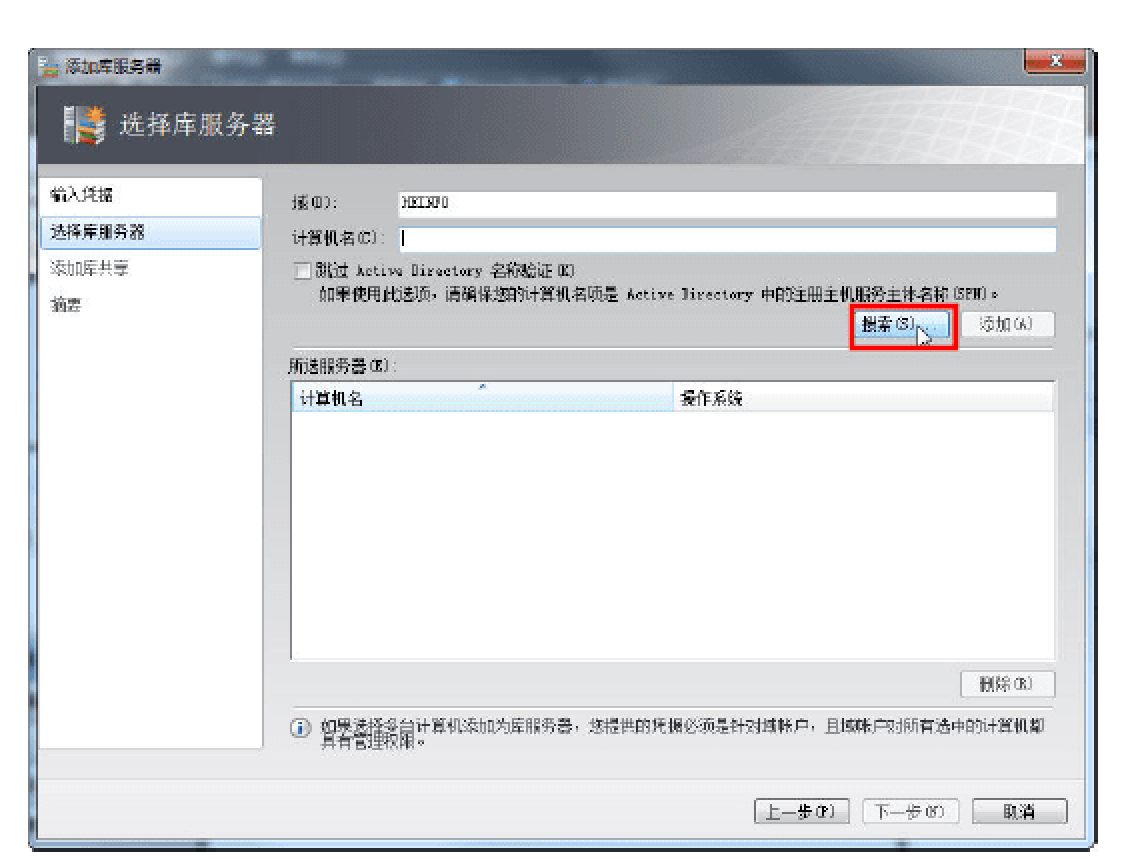


图 12-42 搜索

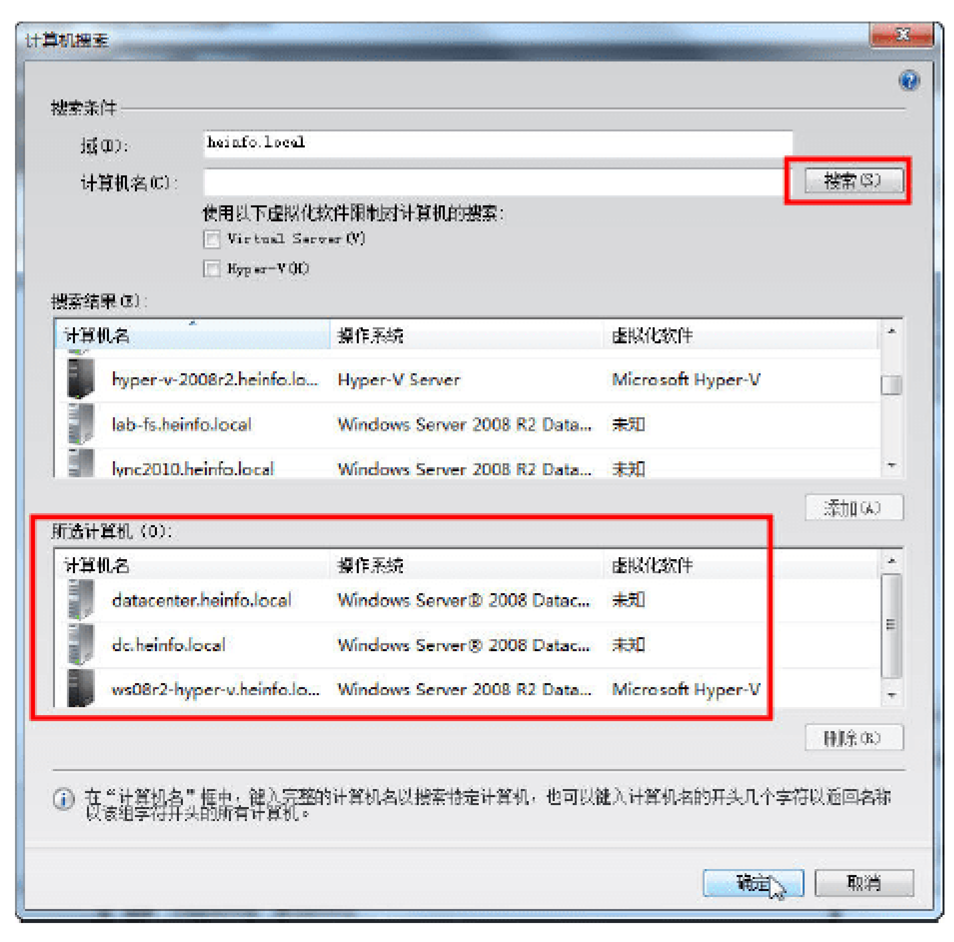


图 12-43 添加计算机到列表

05 返回到“选择库服务器”对话框中，在“所选服务器”列表中已经添加了 3 台主机，如图 12-44 所示。

06 在“添加库共享”对话框中，分别选中保存有操作系统安装光盘镜像文件的共享文件夹，在 2 台域控制器（计算机名称分别为“datacenter.heinfo.local”与“dc.heinfo.local”）中，共享文件夹名称都是“msdn-iso”（这两个文件夹采用 DFS 进行同步），在启用 Hyper-V 功能的 Windows Server 2008 主机中，共享文件夹是 Tools，分别选中各自的共享文件夹（其他的文件夹先不要添加，以后根据需要再进行添加），如图 12-45 所示。

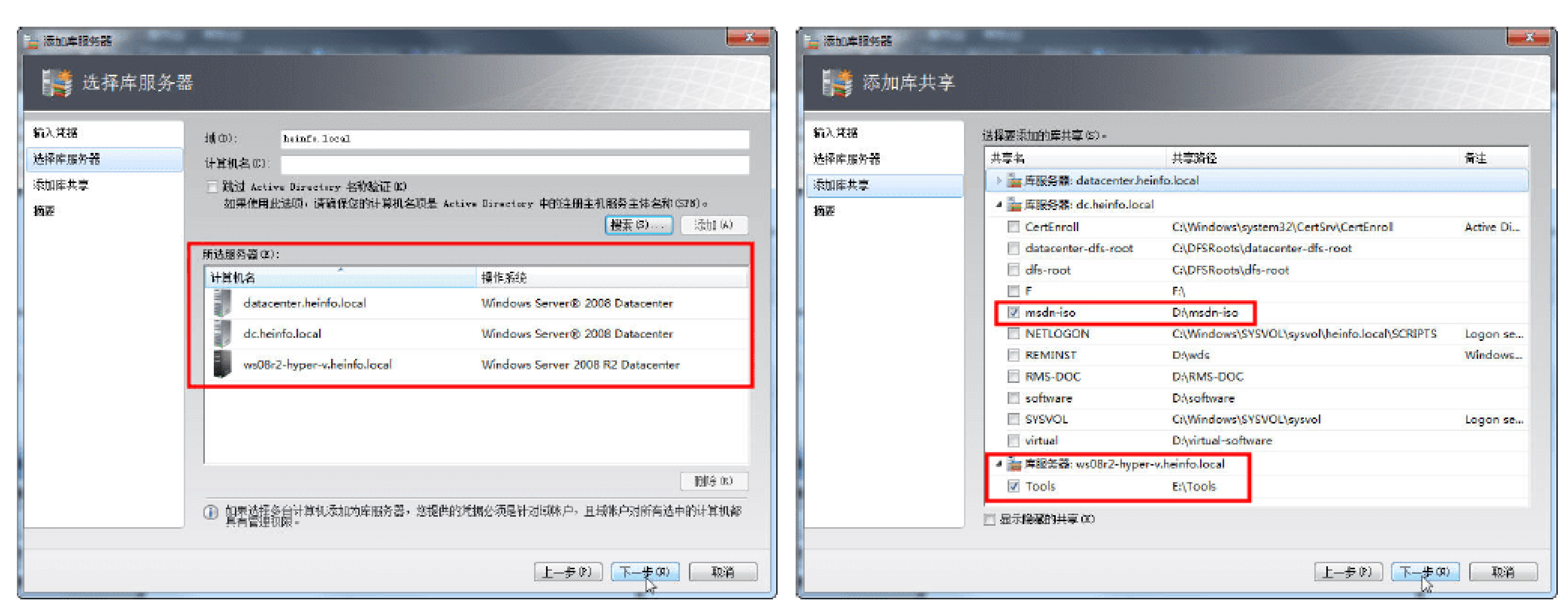


图 12-44　选择库服务器　　　　图 12-45　添加库共享

07 在“摘要”对话框中，显示了添加的库服务器以及添加到库服务器的共享文件夹，无误之后单击“添加库服务器”按钮，如图 12-46 所示。

08 然后弹出“作业”窗口，显示添加的过程，如图 12-47 所示。作业完成之后，关闭这个窗口。

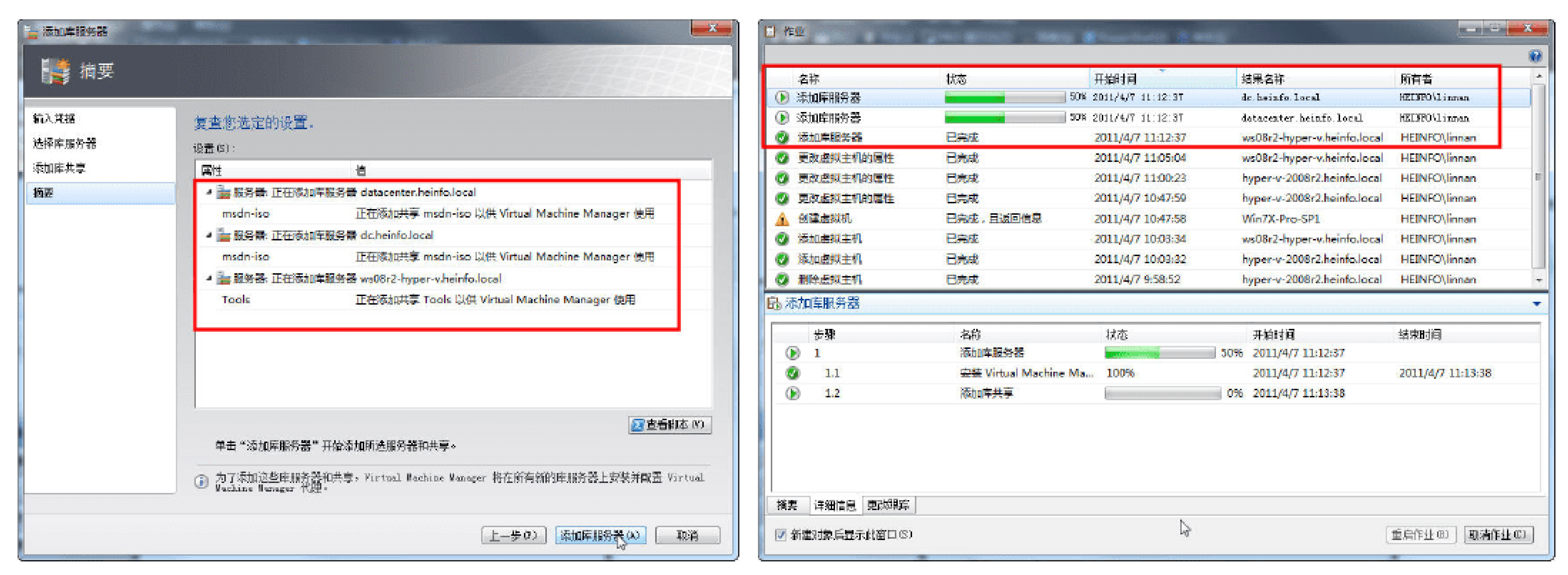


图 12-46　摘要　　　　图 12-47　添加库服务器作业

在添加了具有操作系统镜像的库共享之后，就可以创建虚拟机并在虚拟机中安装操作系统了。

12.3.4　创建虚拟机

在本节的操作中，我们将使用 VMM 管理员控制台，在 Hyper-V Server 2008 R2 主机中，创建一个 Windows Server 2003 虚拟机，然后在虚拟机中安装 Windows Server 2003 操作系统，最后安装 Hyper-V 集成服务。操作步骤如下。

01 使用 VMM 管理员登录到 VMM 服务器，在左侧的任务窗格中选择“虚拟机”，然后在右侧的“操作”窗格中选择“新建虚拟机”链接，如图 12-48 所示。

02 在“选择源”对话框中，在“选择新虚拟机的源”处，选中“使用空白虚拟硬盘创建新的虚拟机”单选按钮，如图 12-49 所示。

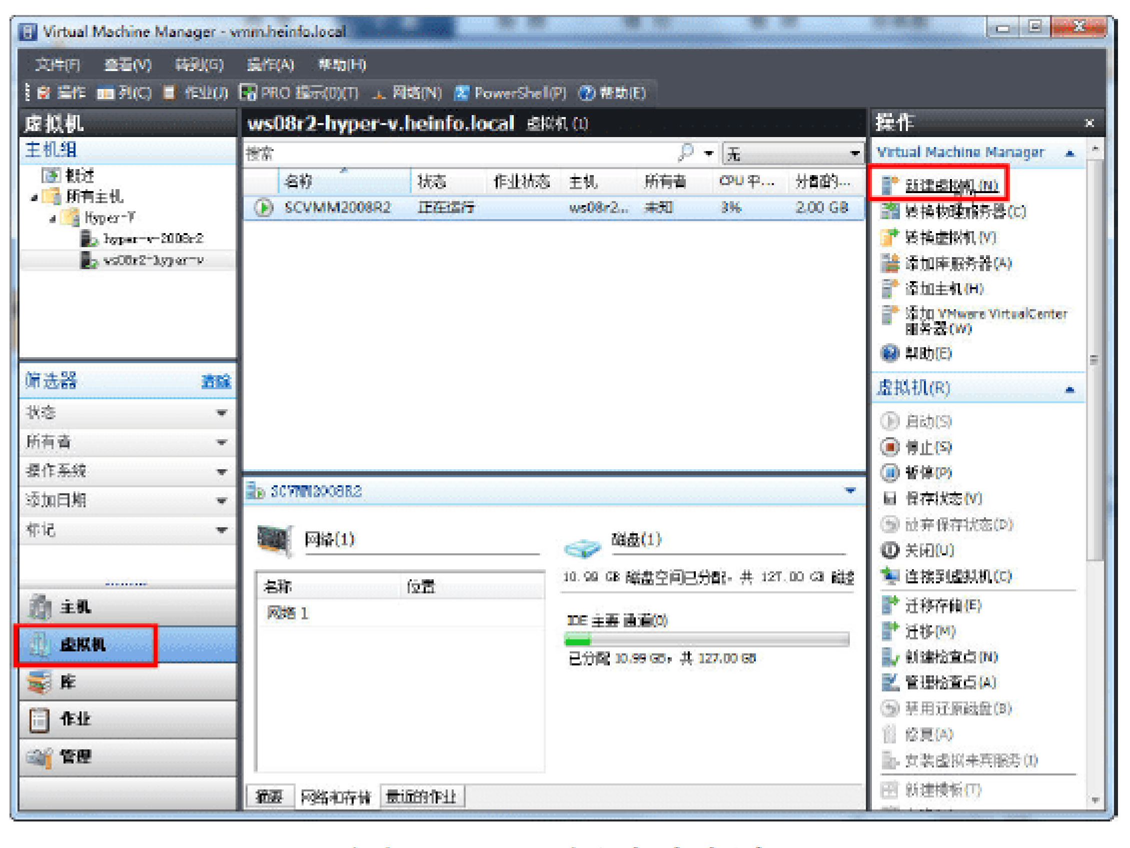


图 12-48　新建虚拟机

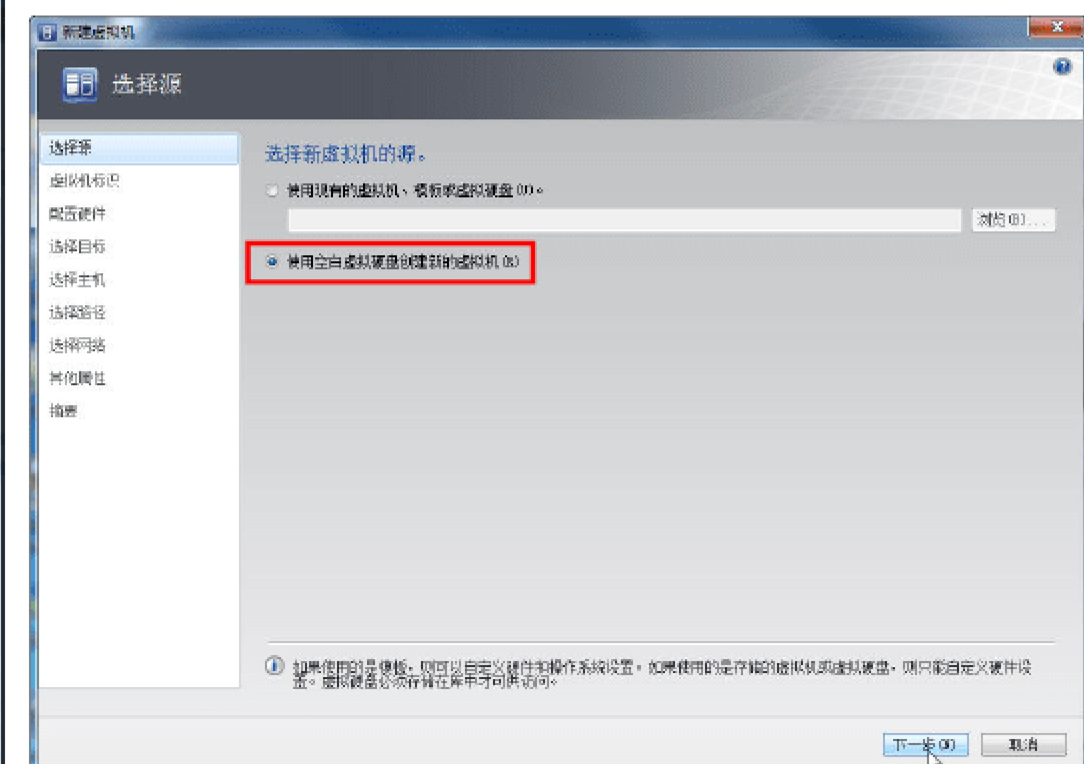


图 12-49　选择源

03 在“虚拟机标识”对话框中，在“虚拟机名称”文本框中，输入欲创建的虚拟机的名称，在本例中为 WS03R2（也可以是其他名称，只要易于分辨，让管理员理解虚拟机的名称及其代表的意义即可），如图 12-50 所示。

04 在“配置硬件”对话框中，选择新建虚拟机的配置，主要是设置 CPU 数量、虚拟机内存、虚拟硬盘大小，以及选择操作系统镜像（用来安装操作系统）。在 Hyper-V 虚拟机中，有个比较有意思的选择，如图 12-51 所示，在“CPU 类型”中，包括了 AMD 与 Intel 两种厂商的服务器的 CPU 型号，这会让初学者理解为，Hyper-V 的虚拟机可以“模拟”这两种型号的 CPU 并能指定 CPU 的频率。实际上，无论你在此选择哪种类型，虚拟机的 CPU 都是与物理主机一致的（可能 CPU 数量不同）。

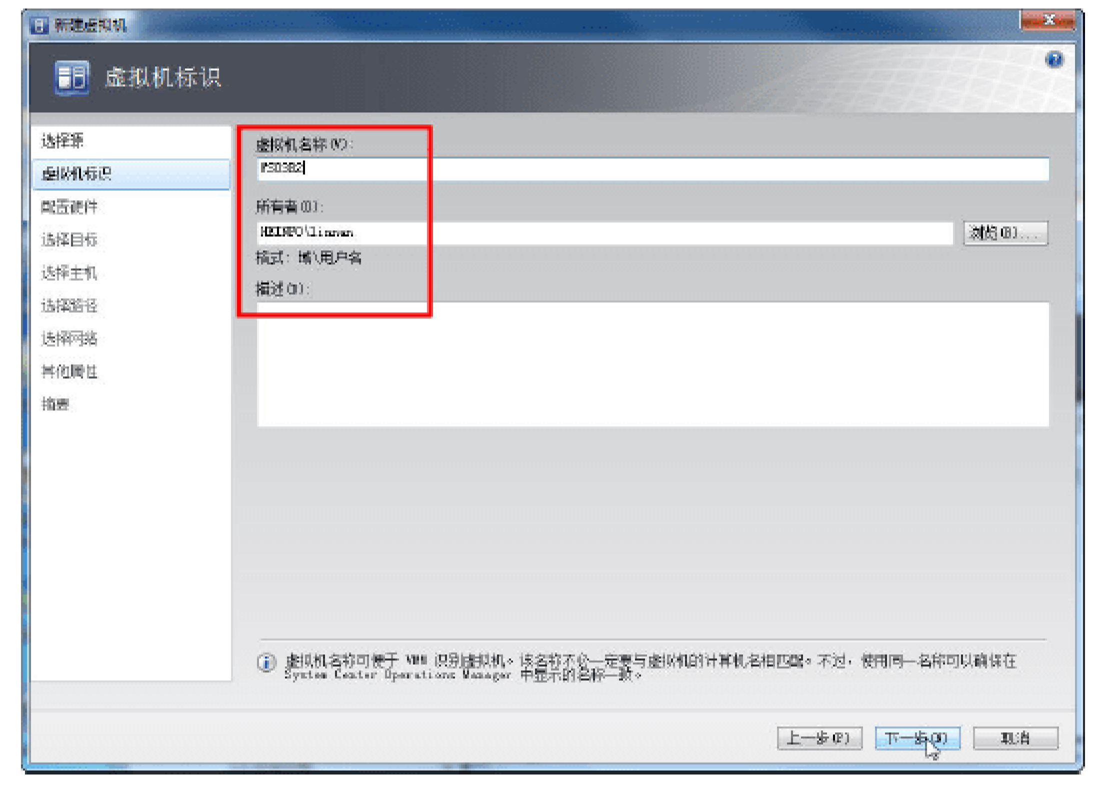


图 12-50　设置虚拟机名称

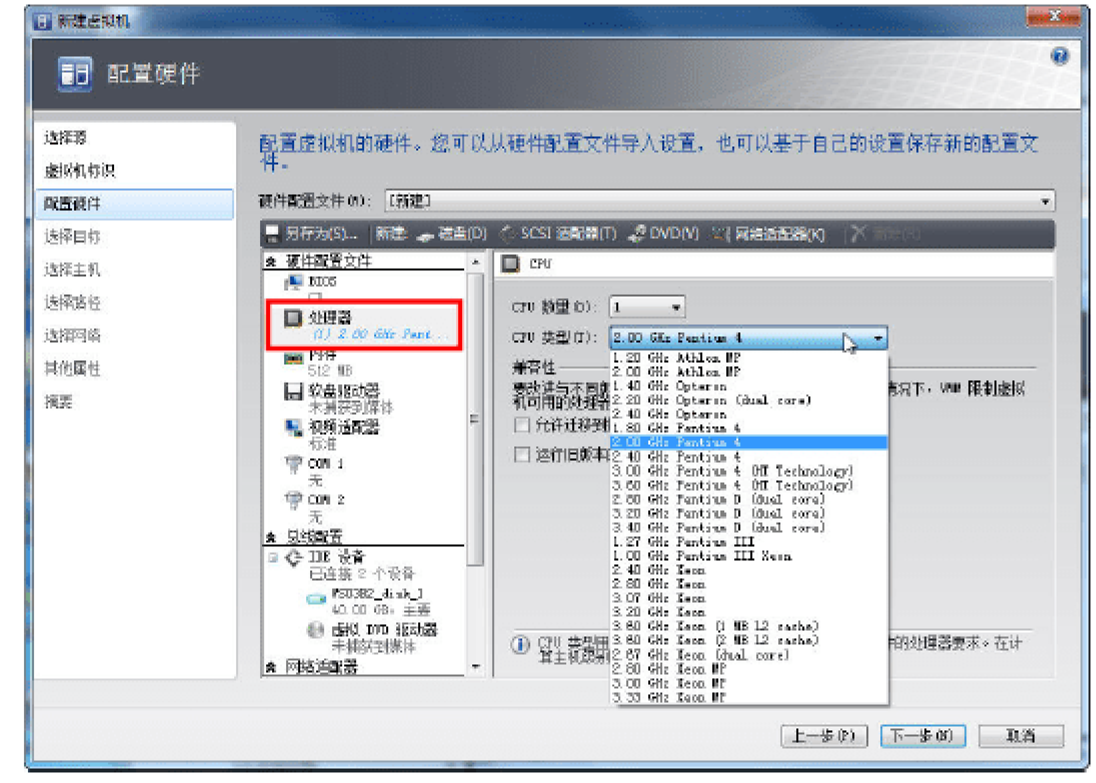


图 12-51　处理器选择

05 在“内存”处为虚拟机分配内存，在 Hyper-V Server 2008 R2 中，已经支持“动态”内存，可以根据需要选择，是为虚拟机分配“静态”内存（内存大小固定），还是分配“动态”内存（设置内存的初始大小以及最大内存），如图 12-52 所示。

06 在“视频适配器”对话框中，选择“标准视频适配器”。如果要体验“Microsoft RemoteFX 3D 视频适配器”，则需要创建 Windows 7 虚拟机，并且在 Windows Server 2008 R2 With SP1 的 Hyper-V 主机中才能使用。

07 在“IDE 设备”处设置虚拟硬盘的类型及大小，如图 12-53 所示。这与在 Hyper-V 中相同。

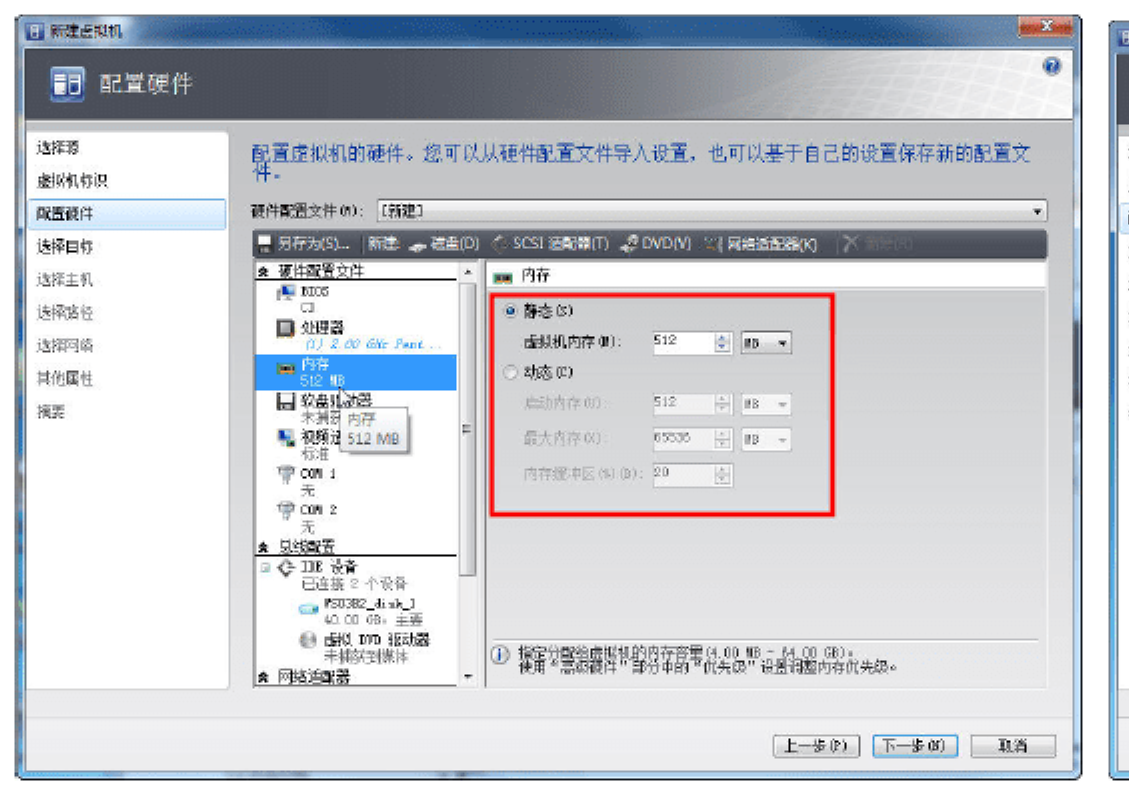


图 12-52　内存

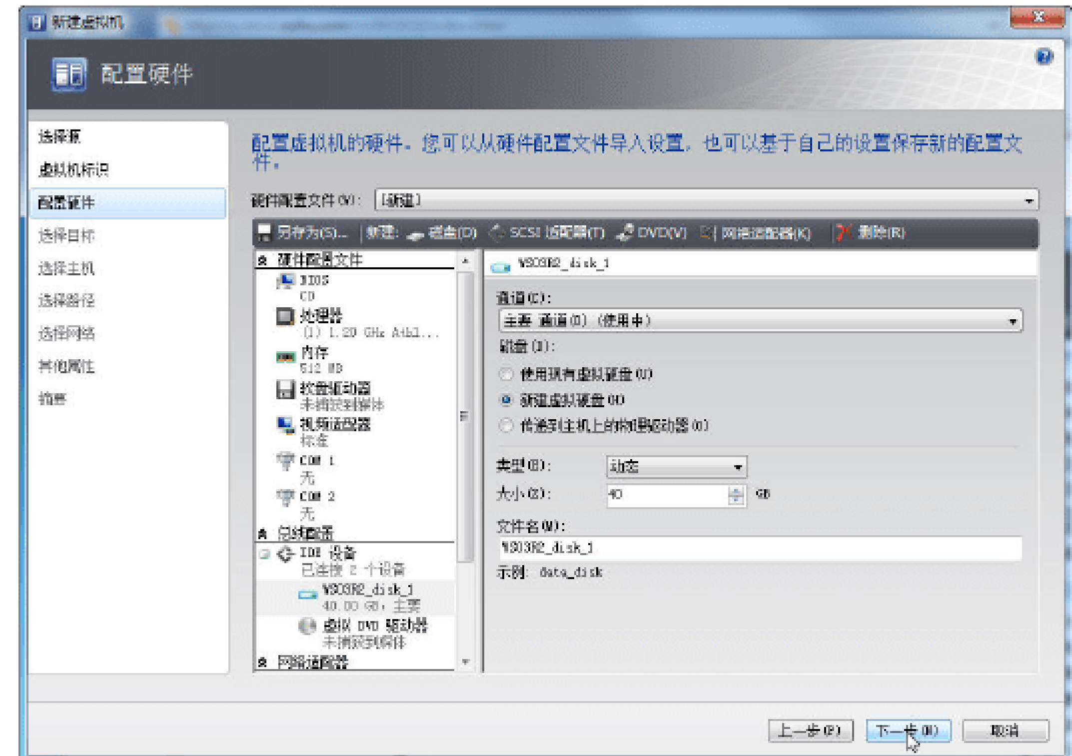


图 12-53　虚拟硬盘大小

08 在“虚拟 DVD 驱动器”处，选中“现有映像文件”单选按钮，然后单击“浏览”按钮（如图 12-54 所示）。在弹出的“选择 ISO”对话框中，选择要映射的镜像文件，如果你的共享库中镜像文件太多，可以输入关键字进行过滤。例如，要选择 Windows Server 2003 的镜像文件，可以输入 Windows 2003，然后列表中会显示所有 Windows 2003 的光盘镜像，如图 12-55 所示。如果是安装 Windows Server 2003 R2，则需要选择第一张光盘镜像文件。

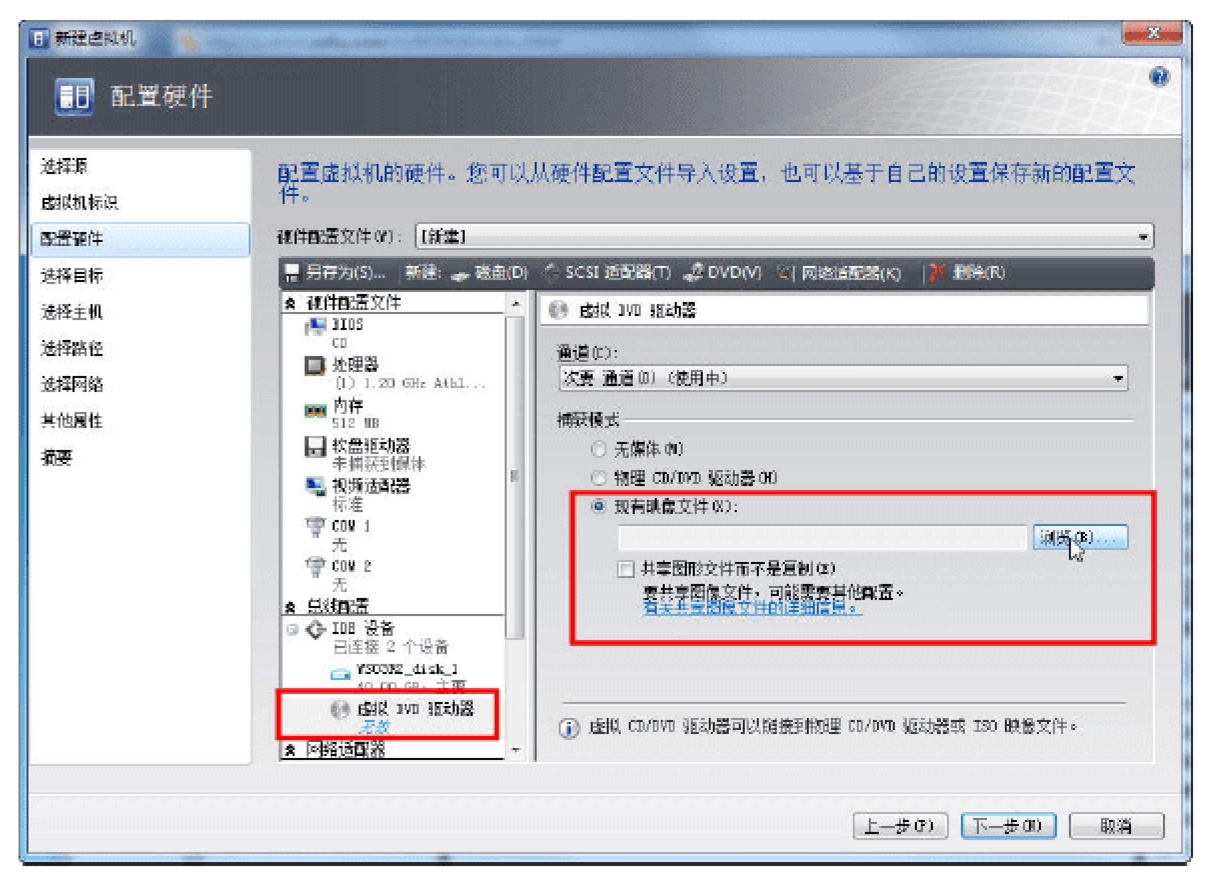


图 12-54　使用映像文件

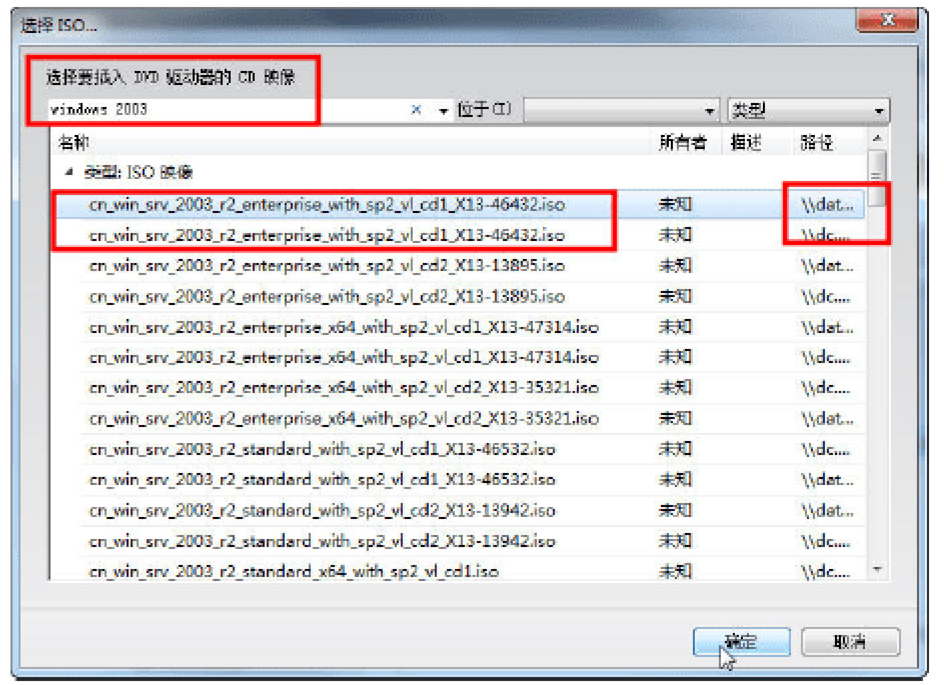


图 12-55　过滤并选择镜像文件

选择之后，返回到“配置硬件”对话框中，如图 12-56 所示，已经以“共享文件夹”的方式选中了镜像文件。

09 在“选择目标”对话框中，选中“将虚拟机放置到主机上”单选按钮，如图 12-57 所示。

10 在“选择主机”对话框中，为虚拟机选择主机，在此选择“hyper-v-2008r2.heinfo.local”，如图 12-58 所示。

11 在“选择目标文件夹”对话框中，选择保存虚拟机的路径，默认情况下是安装 Hyper-V 时选择的路径（默认为 c:\programdata\microsoft\windows\hyper-v），通常情况下，要选择非系统分

区，单击“浏览”按钮，选择前面规划的保存虚拟机的文件夹，在本例中是 D 盘的 Hyper-V 文件夹，如图 12-59 所示。

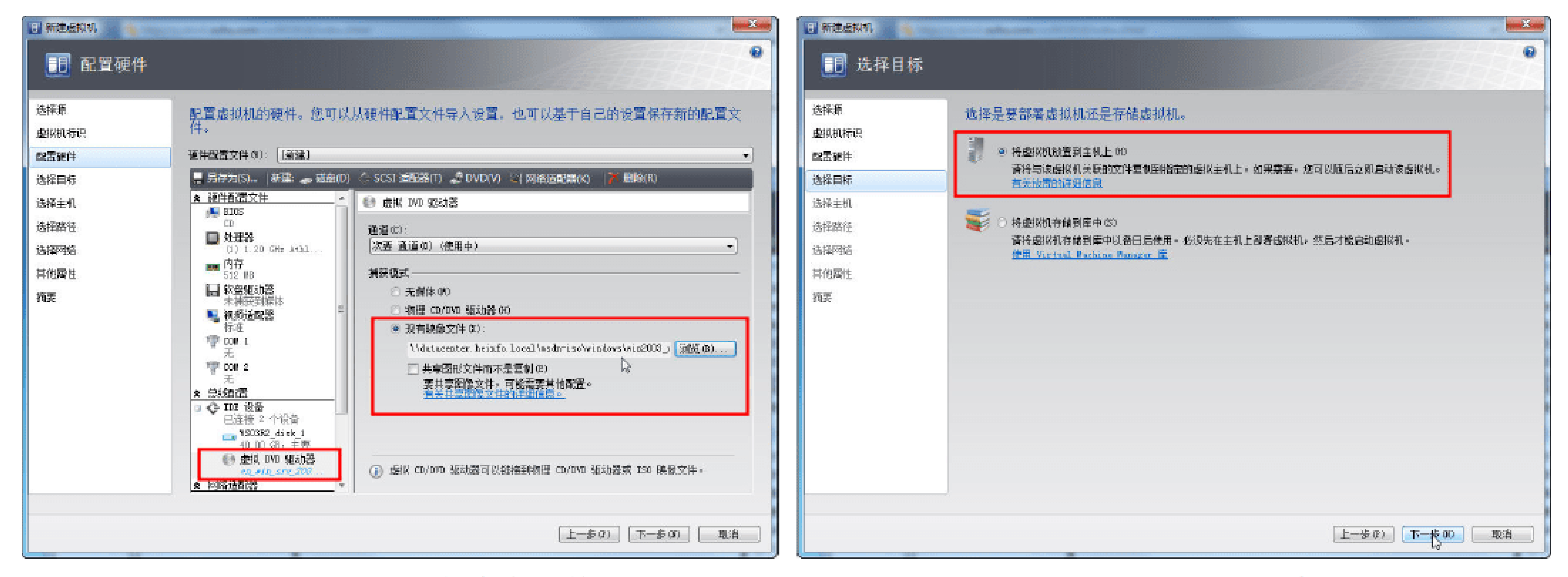
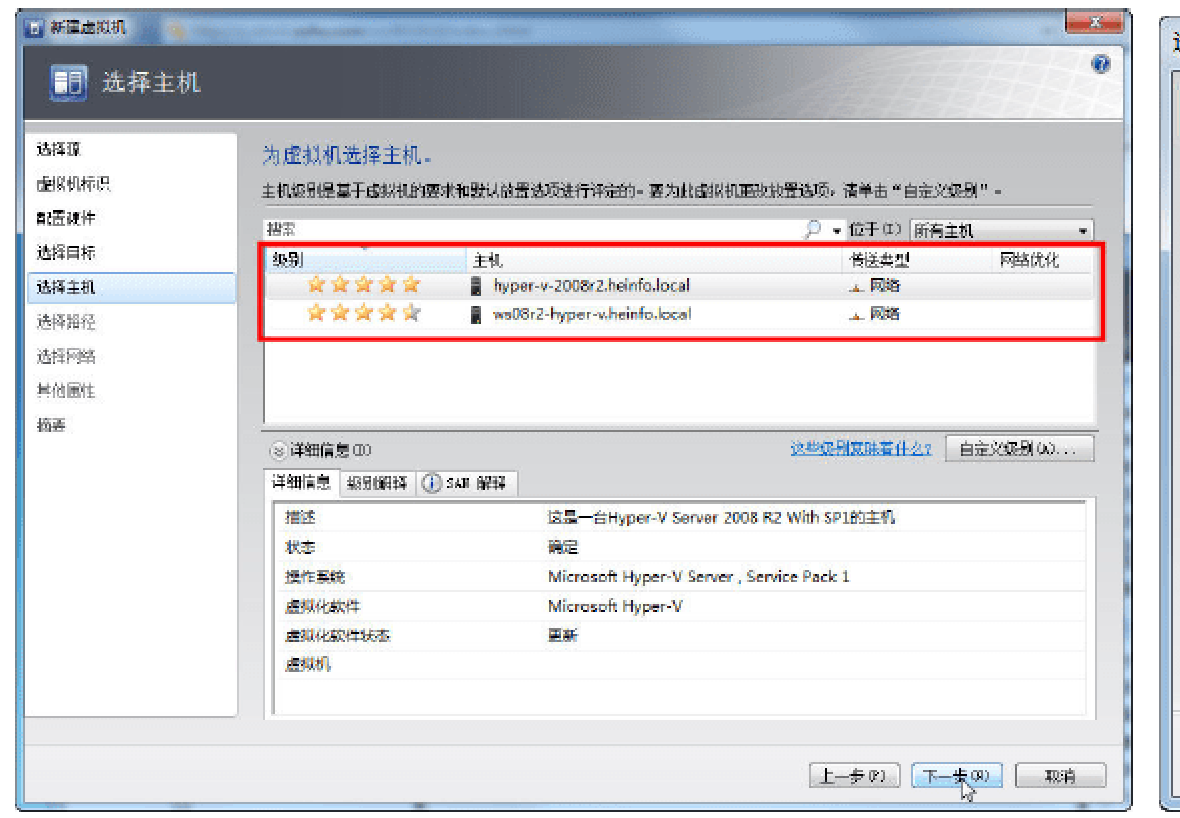


图 12-56　选中镜像文件　　　　图 12-57　选择目标





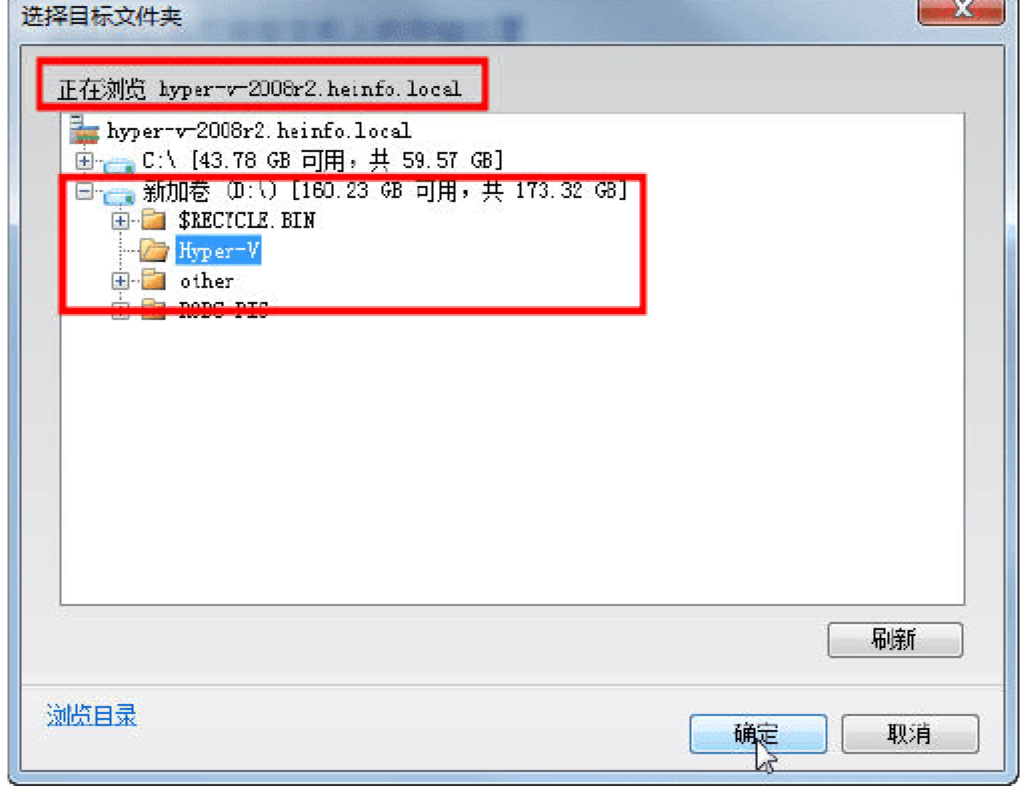


图 12-58　选择主机　　　　图 12-59　浏览选择保存虚拟机的文件夹

选择之后返回到“选择路径”对话框中，并且选中“将此路径添加到主机上的默认虚拟机路径列表”复选框，以后创建虚拟机时，默认将保存在这个文件夹，如图 12-60 所示。如果想要更改，可以单击“浏览”按钮重新进行选择。

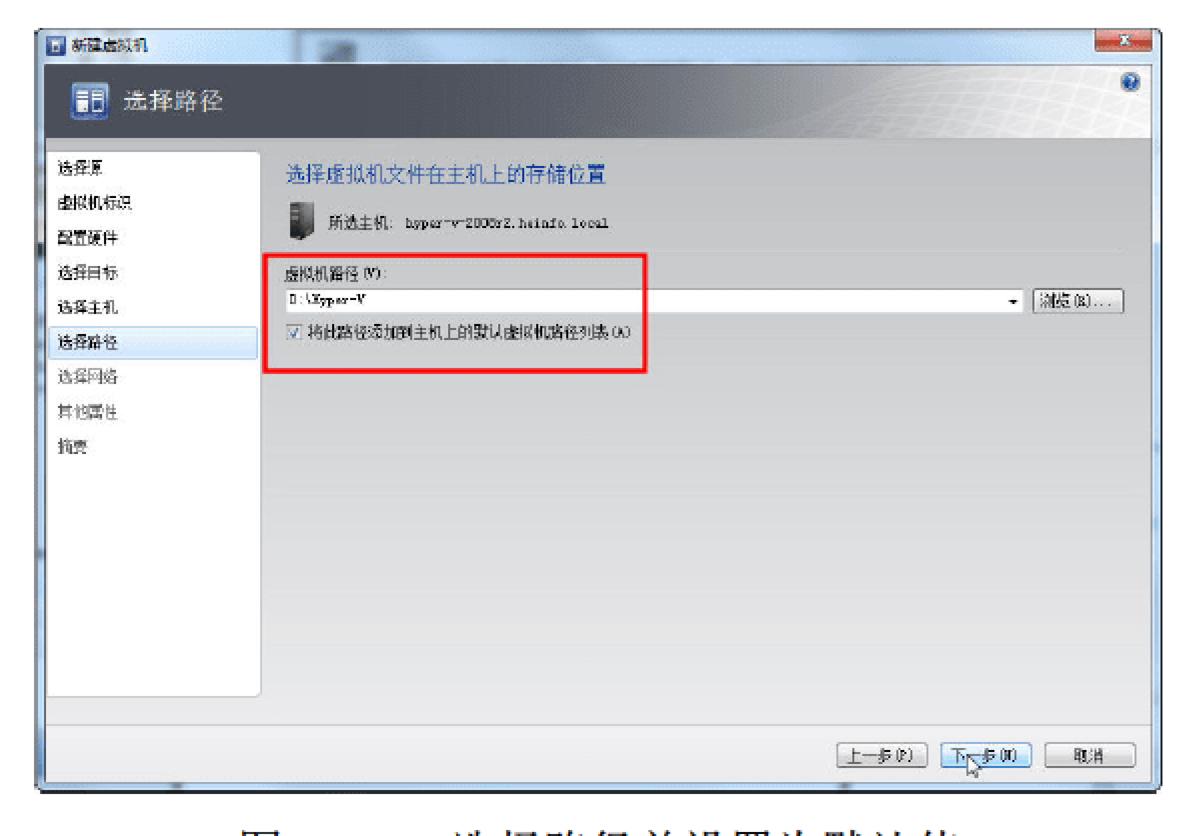


图 12-60　选择路径并设置为默认值

12 在“选择网络”对话框中，为虚拟机选择虚拟网络，如图 12-61 所示。

13 在“其他属性”对话框中，选择虚拟机要安装的操作系统、自动启动操作、信息物理服务器时的操作，在此选择“Windows Server 2003 32 位”，其他根据需要选择，如图 12-62 所示。

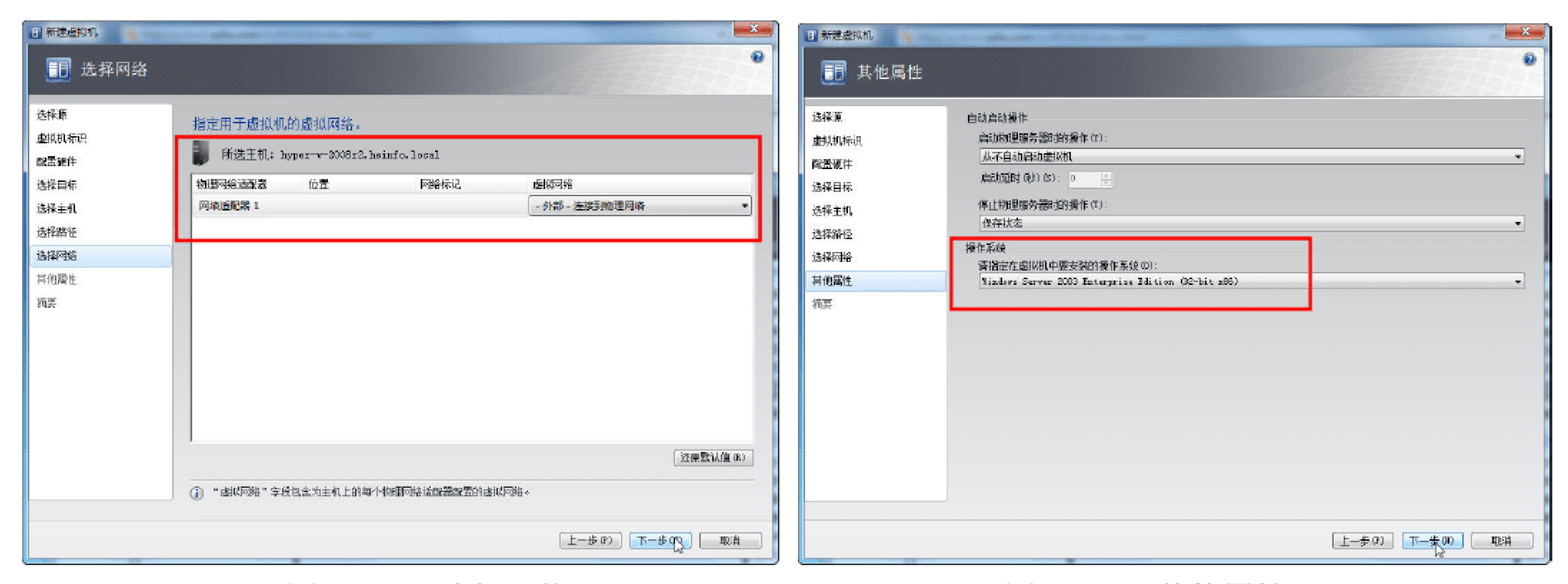


图 12-61　选择网络　　　　图 12-62　其他属性

14 在“摘要”对话框中，复查虚拟机的设置，无误之后，单击“创建”按钮开始创建虚拟机，如果想在创建虚拟机之后启动新创建的虚拟机，则选中“在主机上部署虚拟机之后启动虚拟机”复选框，如图 12-63 所示。

15 在创建虚拟机的“作业”对话框中，如果创建的是 Windows Server 2003，则会出现警告信息，这些并不影响使用，如图 12-64 所示。如果创建的是 Windows Vista 及其以后的虚拟机，则不会出现这些警告信息。在创建完虚拟机后，关闭这个对话框。

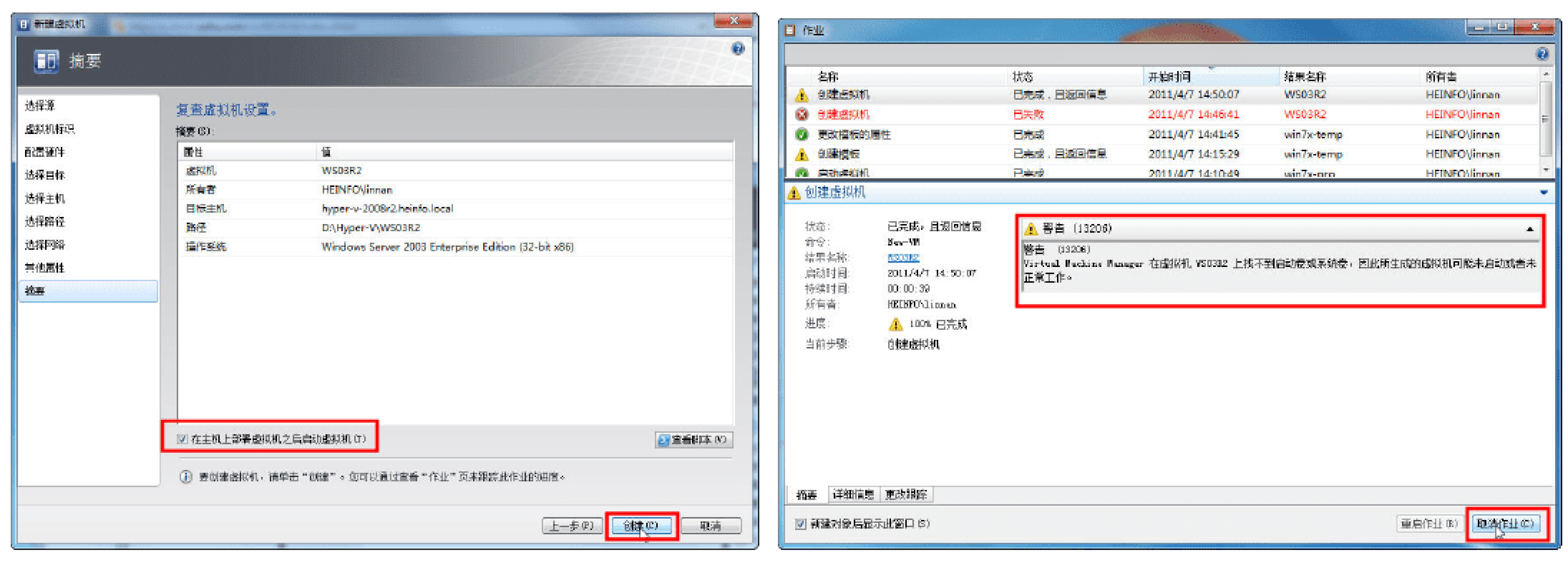


图 12-63 摘要　　　　图 12-64　创建虚拟机作业

12.3.5　在虚拟机中安装操作系统

创建完虚拟机并自动启动之后，接下来连接到虚拟机，开始操作系统的安装，并且在安装完成之后，对虚拟机进行初始配置。主要步骤如下。

01 在 VMM 管理员控制台中，选中新创建的虚拟机，在右侧“操作”窗格中单击“连接到虚拟机”链接，如图 12-65 所示。

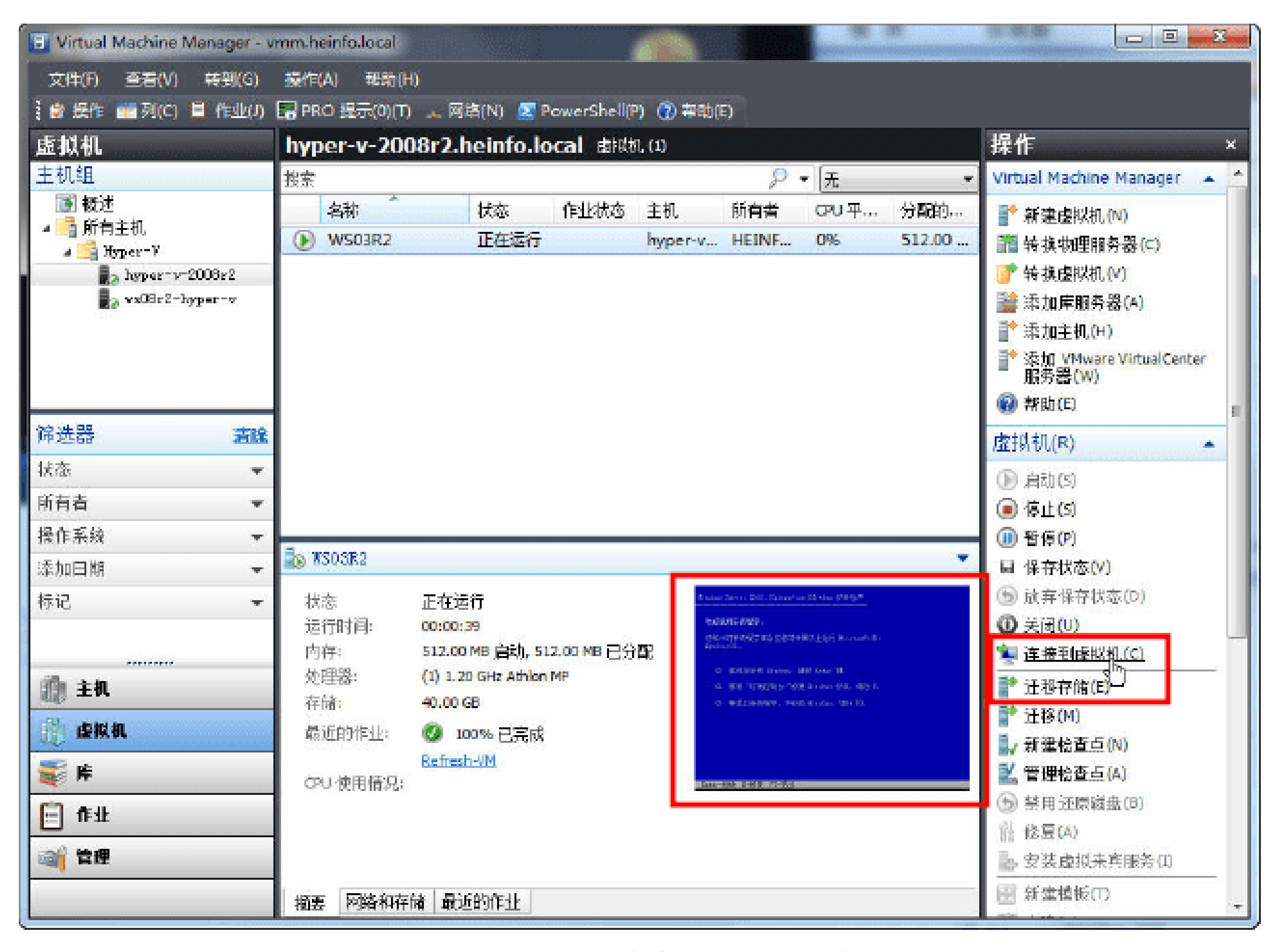
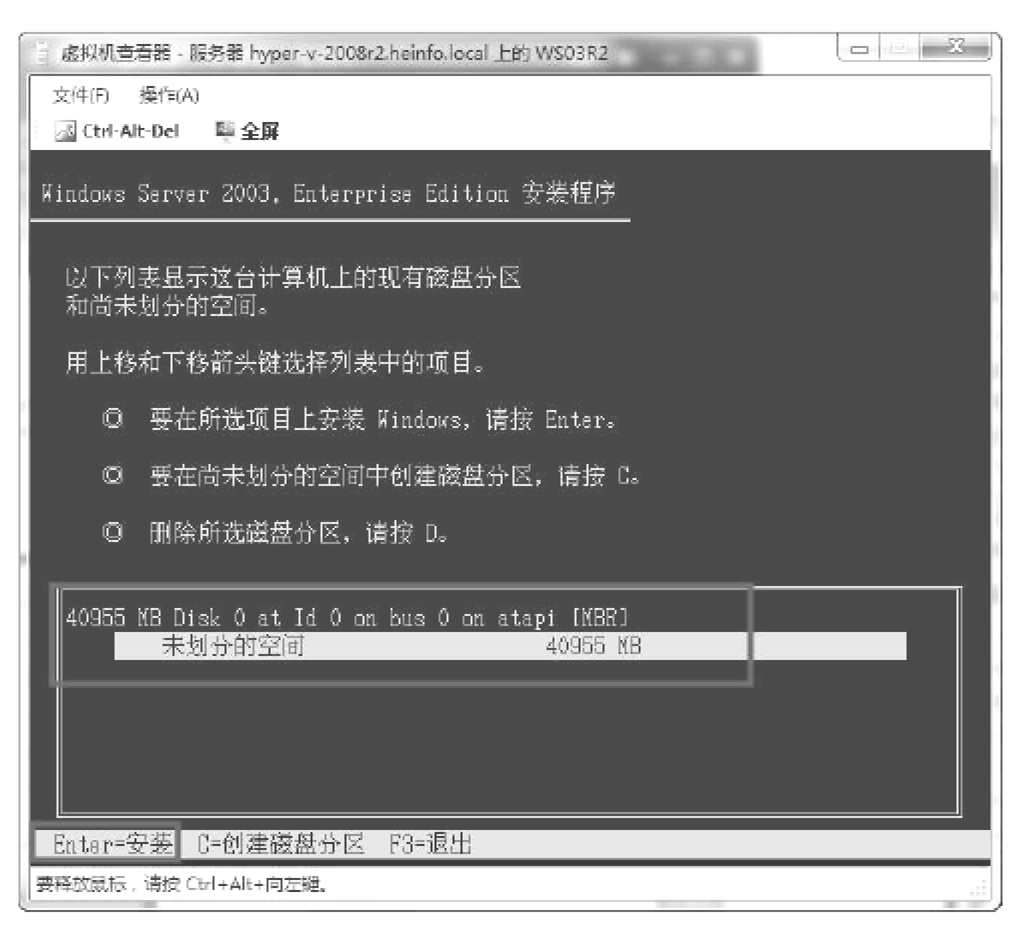


图 12-65　连接到虚拟机

02 连接到虚拟机之后，在“虚拟机查看器”的窗口中，用鼠标单击，进入虚拟机控制窗口，安装操作系统。在创建 Windows Server 2003 虚拟机的时候，默认的虚拟硬盘是 40GB，如果创建的虚拟机用于实际的需要，可将这 40GB 的空间划分为一个分区，所以，直接在磁盘选择页按回车键即可，如图 12-66 所示。

03 使用 NTFS 文件系统格式化，如图 12-67 所示。



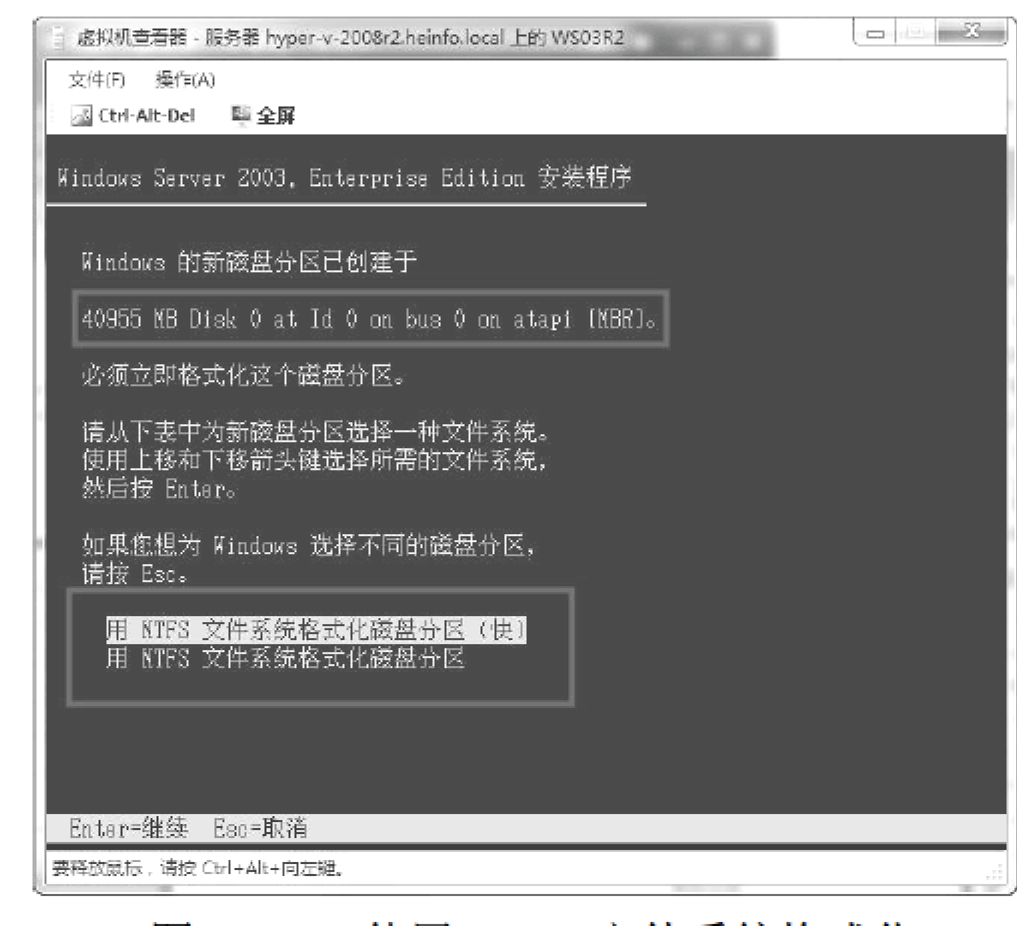


图 12-66　选择分区　　　　图 12-67　使用 NTFS 文件系统格式化

04 在“自定义软件”对话框中，输入用户信息，如图 12-68 所示。

05 在“授权模式”对话框中，选中“每服务器”单选按钮，并设置并发连接数，请根据情况设置，如图 12-69 所示。

06 在安装完成之后，进入 Windows Server 2003 界面。如果安装的是 Windows Server 2003 R2，则安装程序会提示插入第 2 张安装光盘，如图 12-70 所示。

07 如果要更换安装光盘，须返回到 VMM 管理员控制台，用鼠标右击虚拟机，在弹出的快捷菜单中选择“属性”命令，如图 12-71 所示。

图 12-68 用户信息



图 12-69 设置授权模式

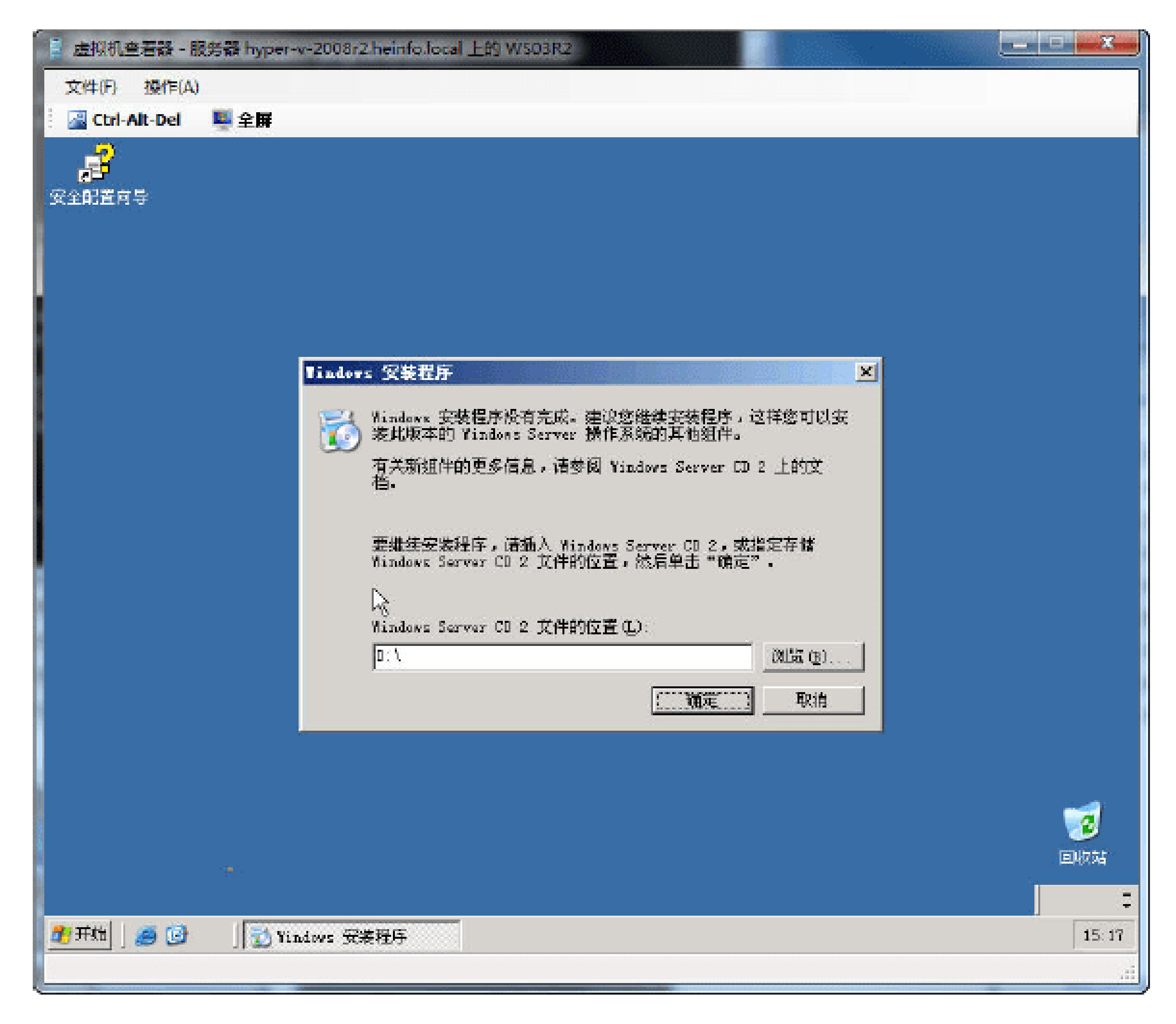


图 12-70 插入第 2 张盘



图 12-71 属性

08 在“虚拟机 属性”对话框中，在“硬件配置”选项卡中，在“虚拟 DVD 驱动器”选项中，单击“浏览”按钮，如图 12-72 所示。

09 在弹出的“选择 ISO”对话框中，选择 Windows Server 2003 R2 的第 2 张光盘镜像，如图 12-73 所示。

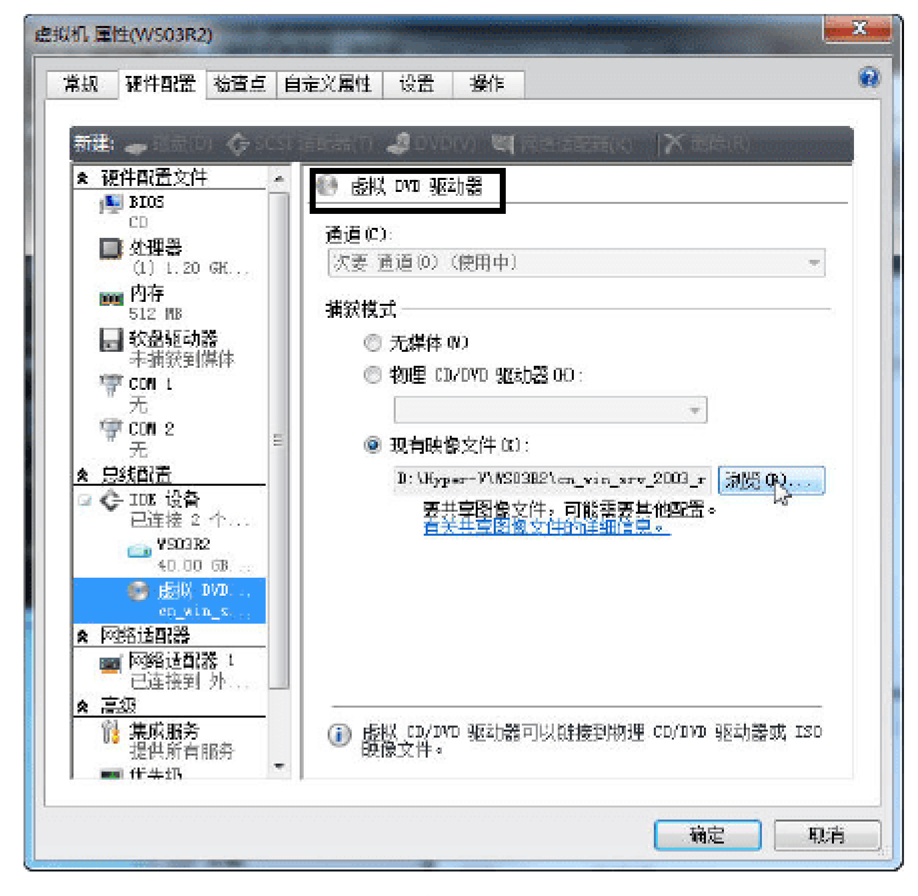


图 12-72 虚拟 DVD 驱动器

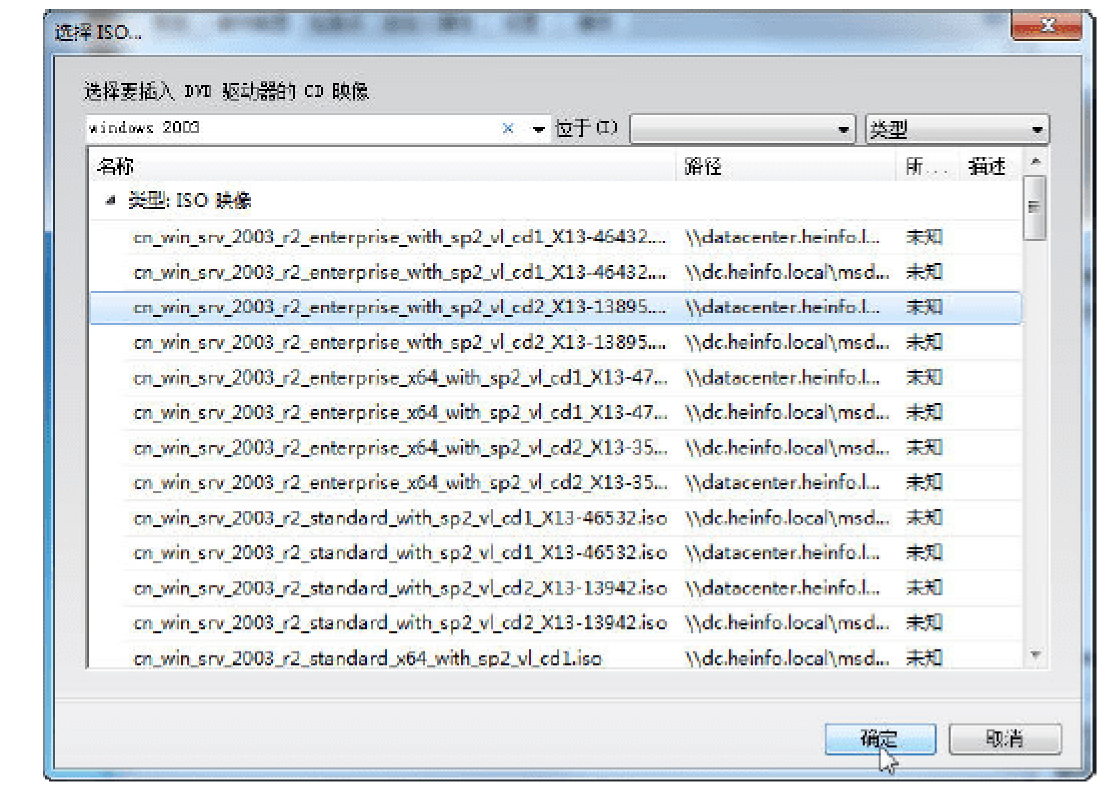


图 12-73 选择 ISO

10 选择之后，单击两次“确定”按钮返回，然后返回到“虚拟机查看器”，继续 Windows Server 2003 R2 的安装，如图 12-74 所示。

11 安装完成后（如图 12-75 所示），以正常的方式关闭虚拟机操作系统（单击“开始”菜单选择“关闭系统”）。

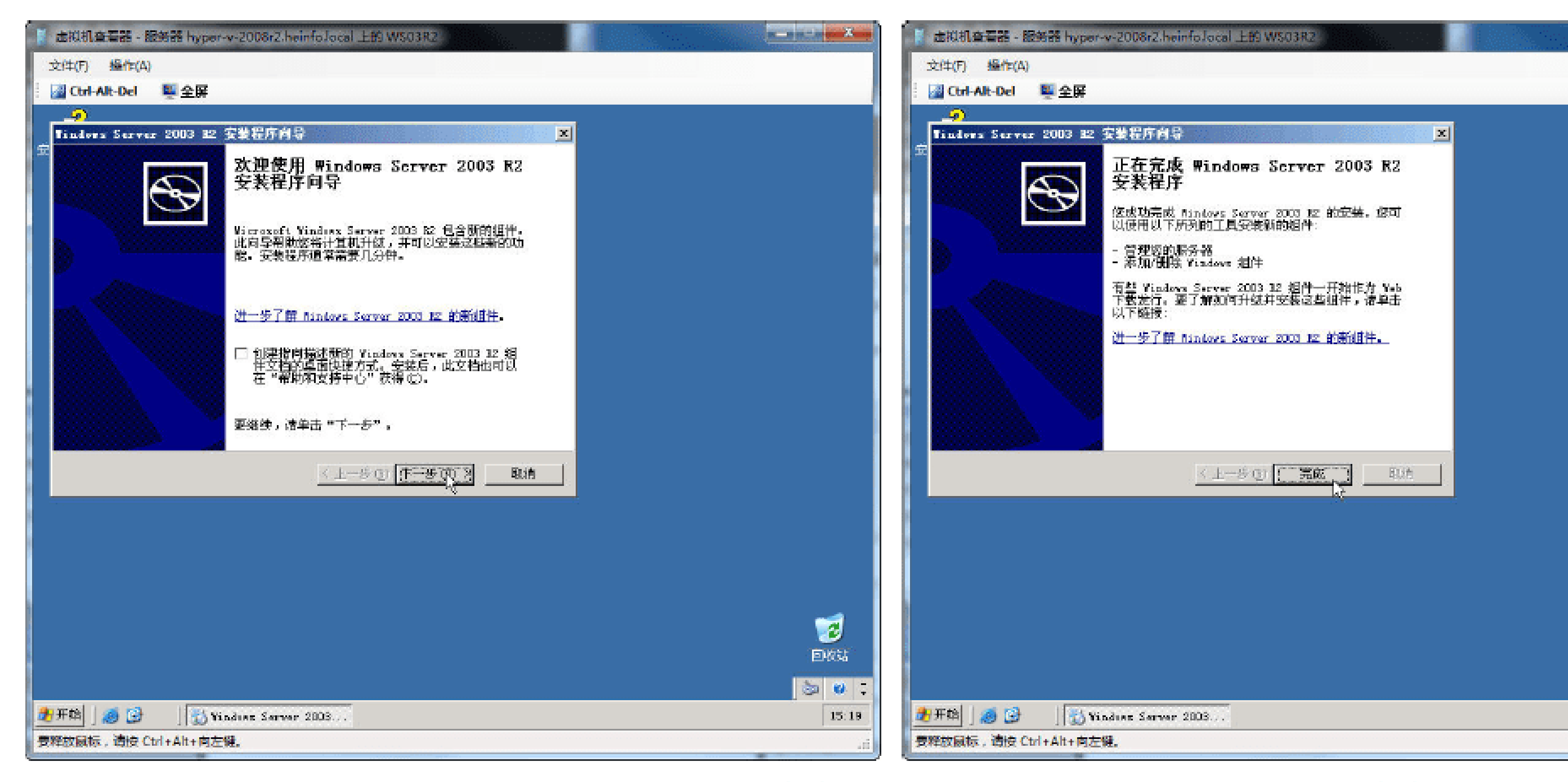


图 12-74 继续 Windows Server 2003 R2 的安装　　图 12-75 安装完成

12 当虚拟机停止后，用鼠标右击，在弹出的快捷菜单中选择“安装虚拟来宾服务”，如图 12-76 所示。这与 Hyper-V 不同，Hyper-V 虚拟机需要在启动的时候安装“集成服务”，而 VMM 管理的虚拟机，则需要在“关机”之后安装。

13 在安装的过程中，在 VMM 管理员控制台会有进度提示，如图 12-77 所示。

14 安装完成之后，可以启动虚拟机，进行后续的工作，如图 12-78 所示。

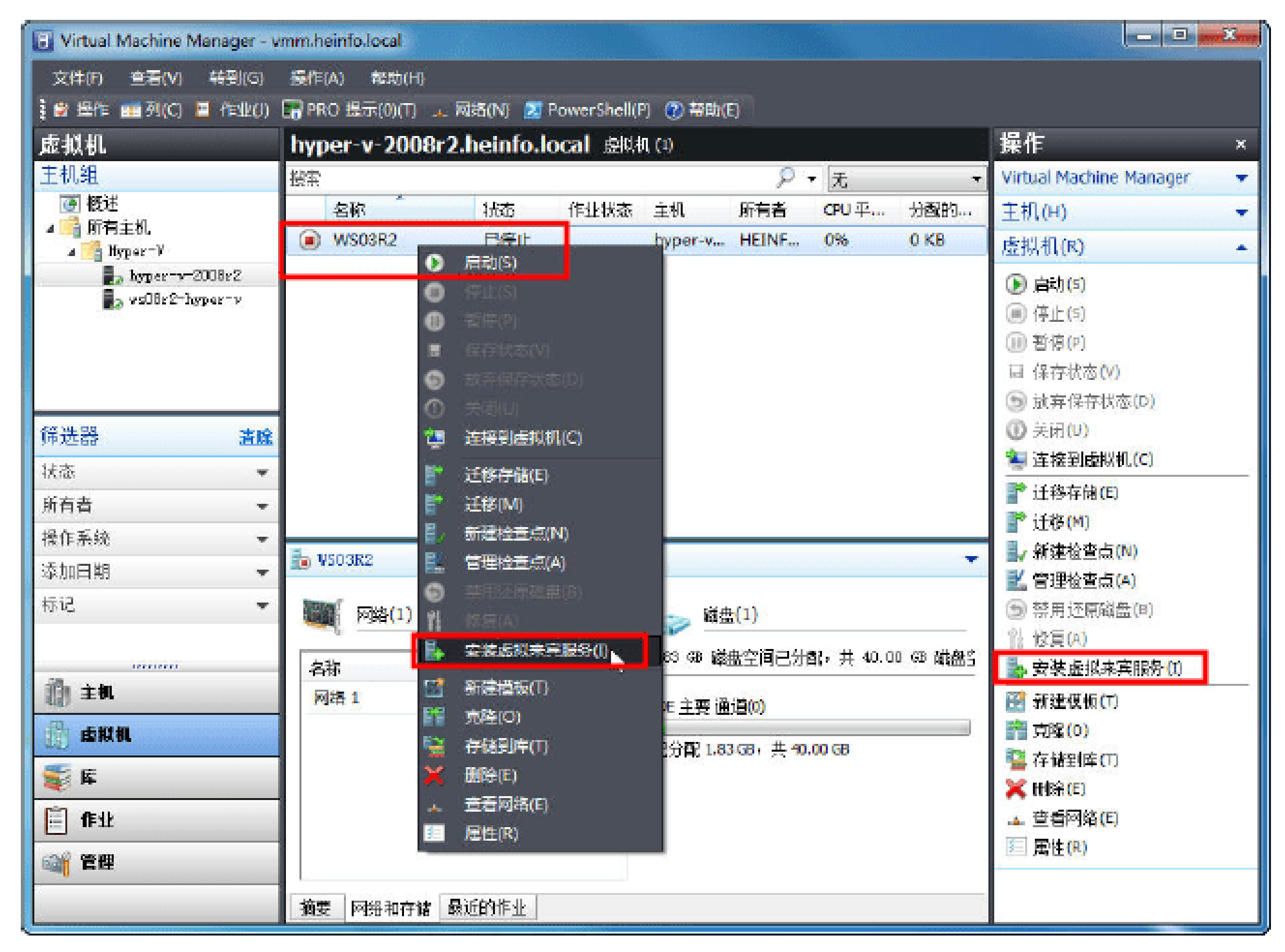


图 12-76　安装虚拟来宾服务

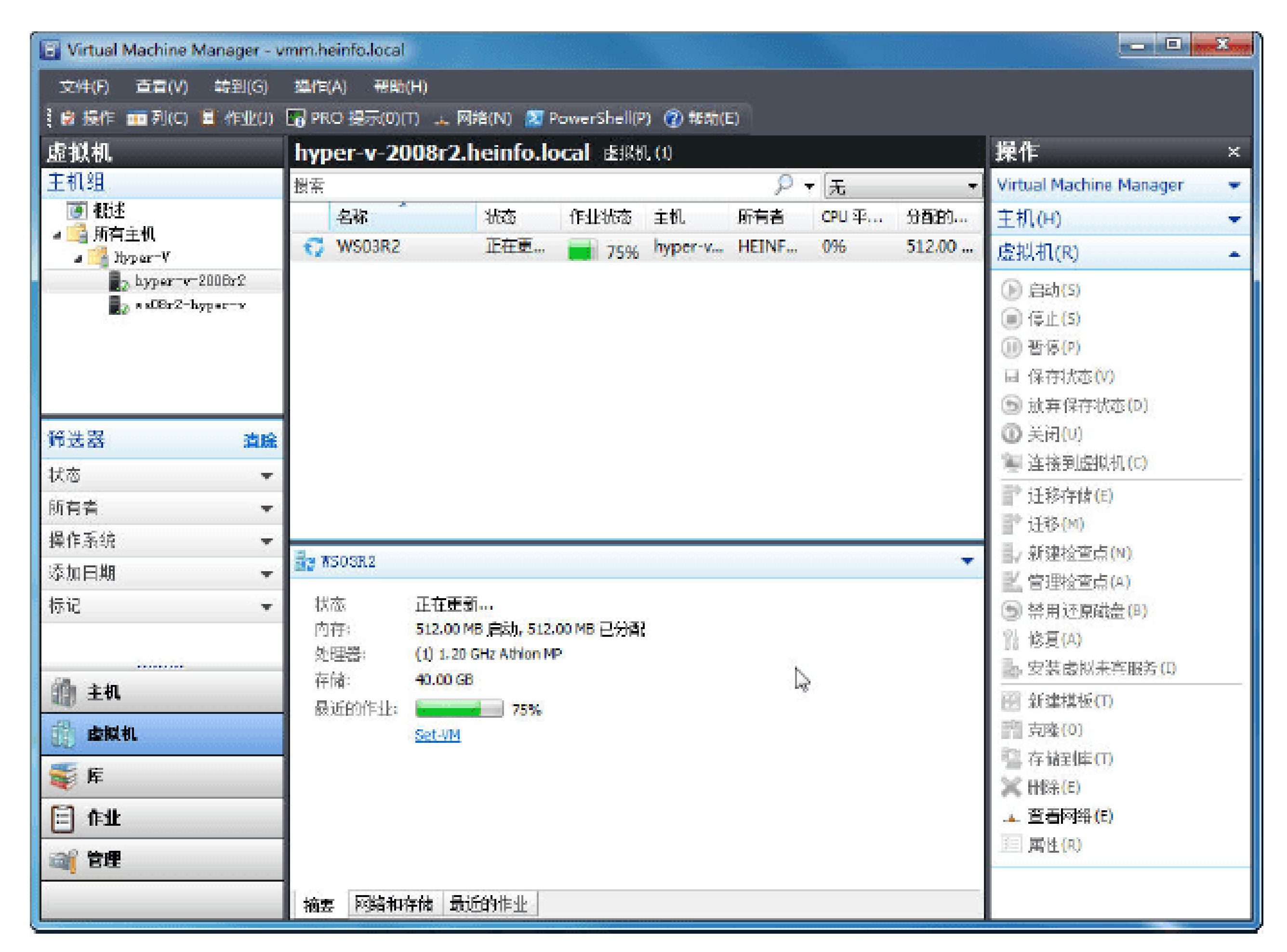


图 12-77　安装进度



图 12-78　启动虚拟机

12.4 在 SCVMM 中使用模板部署虚拟机

在前面的文章中，我们介绍了在 VMM 中创建虚拟机，在虚拟机中安装操作系统等内容，可以发现，这和在 Hyper-V 上创建虚拟机，然后在虚拟机中安装操作系统区别不大。如果需要“批量”部署虚拟机，怎么才能体现出 VMM 的优势呢？这就需要用到 SCVMM 的“模板”功能。在本节中，将介绍怎样从一个“基础”虚拟机转换成模板，并以此模板为基础，使用简单的方法与步骤部署虚拟机。

12.4.1 添加保存模板的库共享文件夹

在 VMM 中，需要将模板保存在“库”共享中。可以在 Hyper-V 主机中创建一个让 Administrator 组具有“完全控制”权限的共享文件夹，并将此共享文件夹添加到库中，供模板虚拟机使用。

在本节的内容中，将在 2 台 Hyper-V 主机中分别创建共享文件夹，然后将这 2 个共享文件夹添加到库共享中。创建共享文件夹的步骤如下。

01 在 172.30.5.31 的主机中，或者使用“远程桌面”登录到 172.30.5.31，在 E 盘创建 MSVM-TEMP 文件夹，并将此文件夹设置为共享文件夹，允许 Administrators 组“完全控制”，如图 12-79 所示。

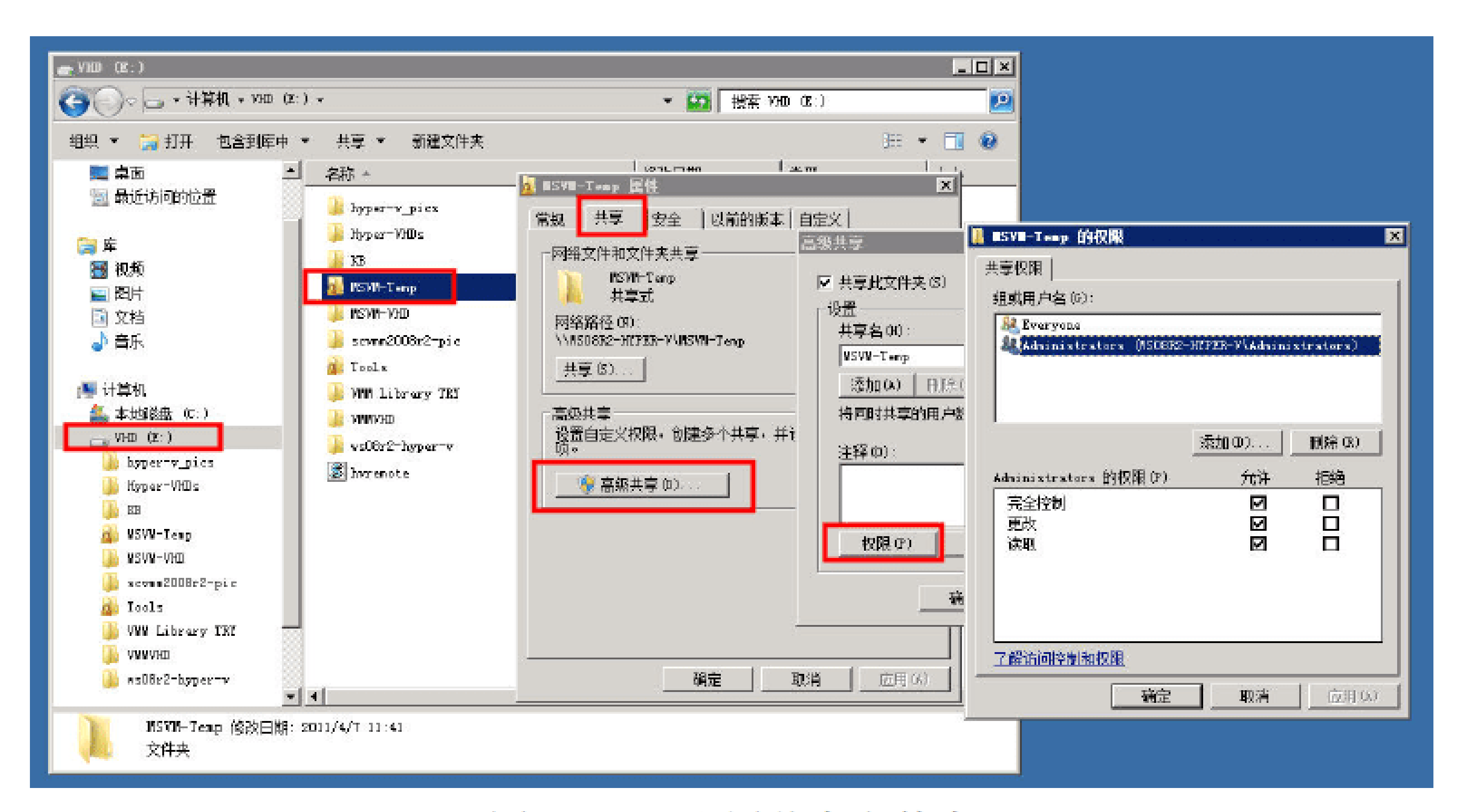


图 12-79 配置共享文件夹

02 对于另一台 Hyper-V 主机，由于没有图形管理界面，所以，可以在网络中的另一台 Windows Server 2008 主机中使用 MMC 管理控制台，添加 “计算机管理”组件，在添加的时候，选择“远程计算机”并指定 Hyper-V 主机的 IP 地址为 172.30.5.17，这样就可以使用图形界面管理远程 Hyper-V 主机了。

添加之后，在“计算机管理→系统工具→共享文件夹→共享”中，创建共享，共享名为 MSVM-Temp-Hyper-V，该共享指向 172.30.5.17 的 D 盘 MSVM-Temp-Hyper-V 文件夹，如图 12-80 所示。

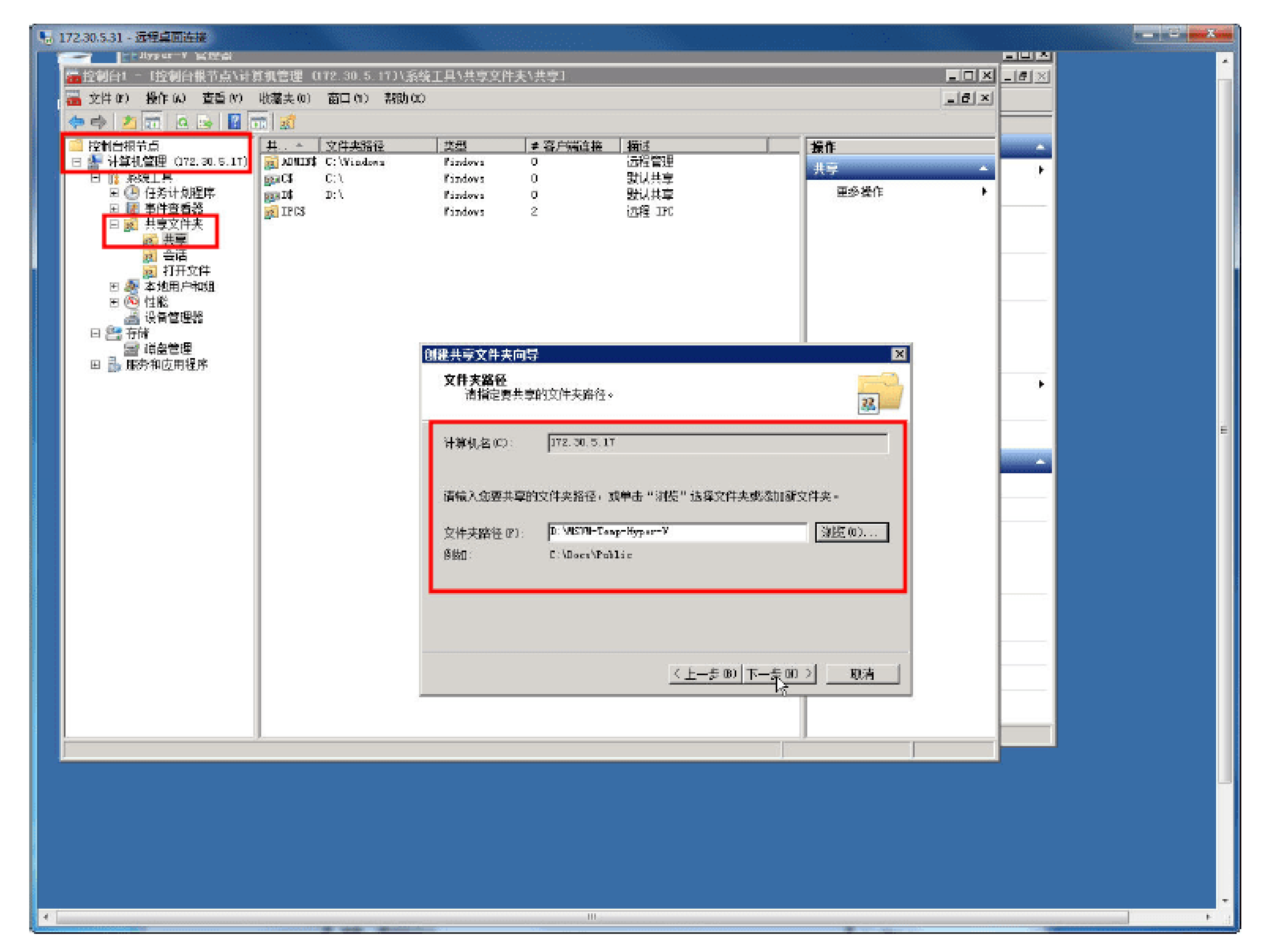


图 12-80　创建共享

在创建的时候，允许“管理员组”具有完全控制权限，其他用户有只读权限，如图 12-81 所示。共享成功之后，单击“完成”按钮，如图 12-82 所示。

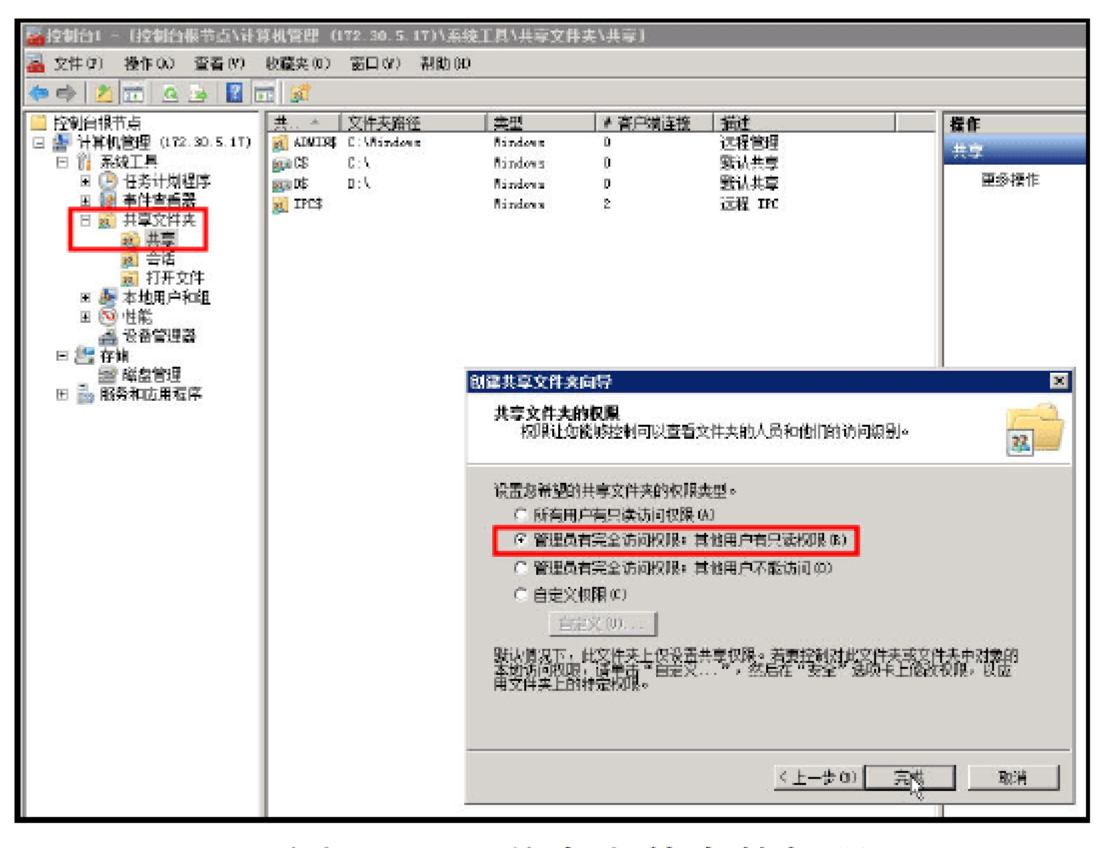


图 12-81　共享文件夹的权限

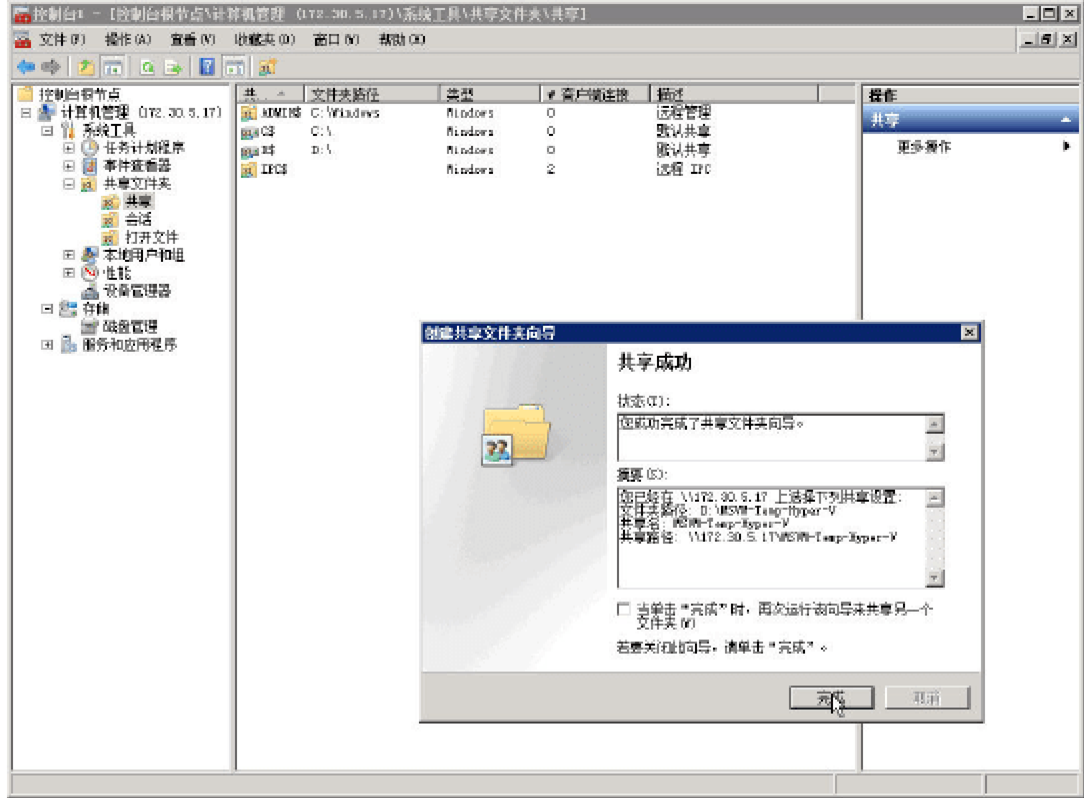


图 12-82　共享成功

在 2 台主机上创建共享文件夹之后，接下来将这两个共享文件夹添加到“库”服务器上，步骤如下。

01 在 VMM 管理员控制台中，在左侧的任务窗格中选中“库”，然后右击“hyper-v-2008r2.heinfo.local”库服务器，在弹出的快捷菜单中选择“添加库共享”命令，如图 12-83 所示。

02 在“添加库共享”对话框中，选中前面创建的共享文件夹，如图 12-84 所示。

03 在“摘要”对话框中，复查设置，如图 12-85 所示。

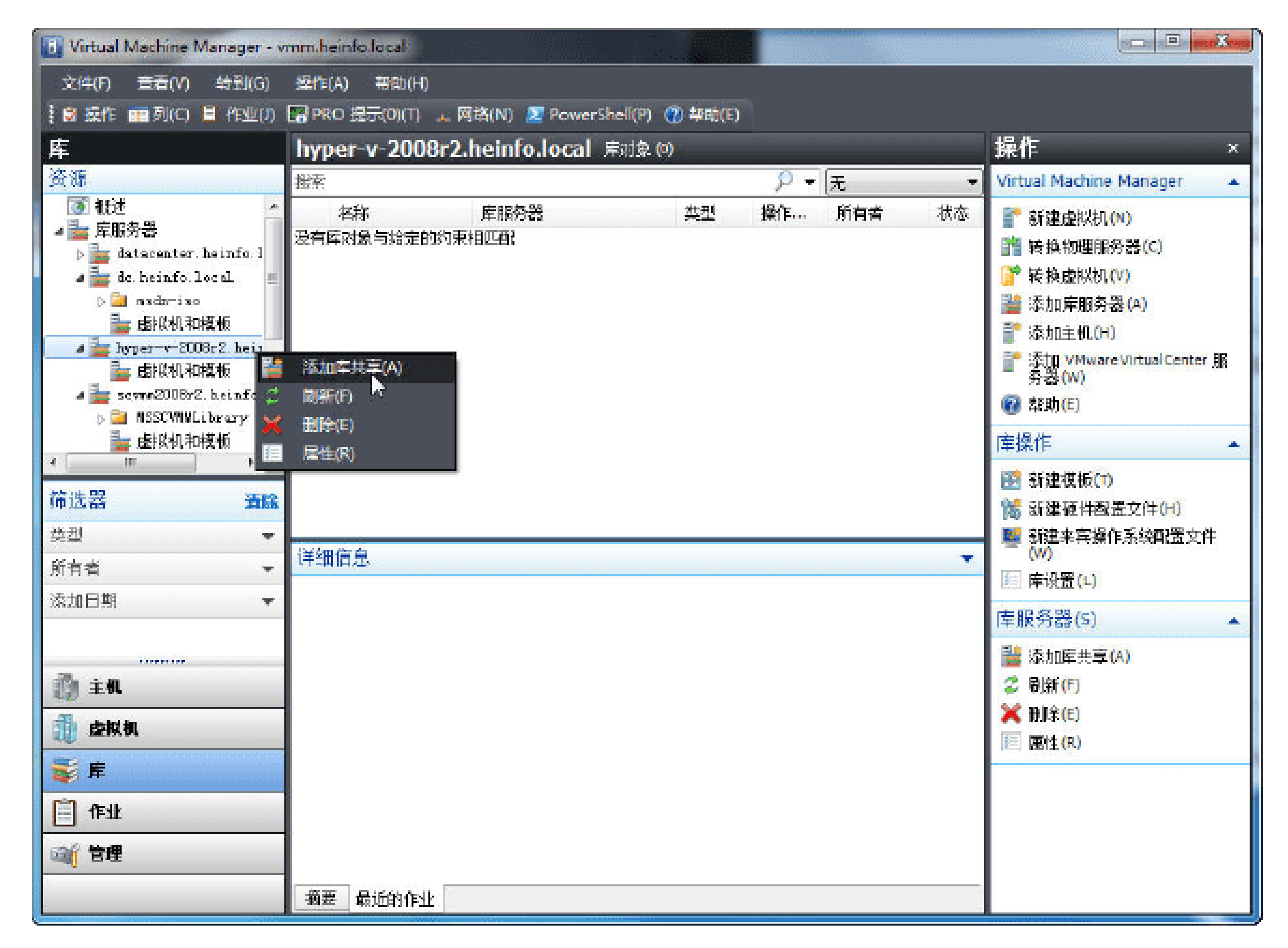


图 12-83　添加库共享

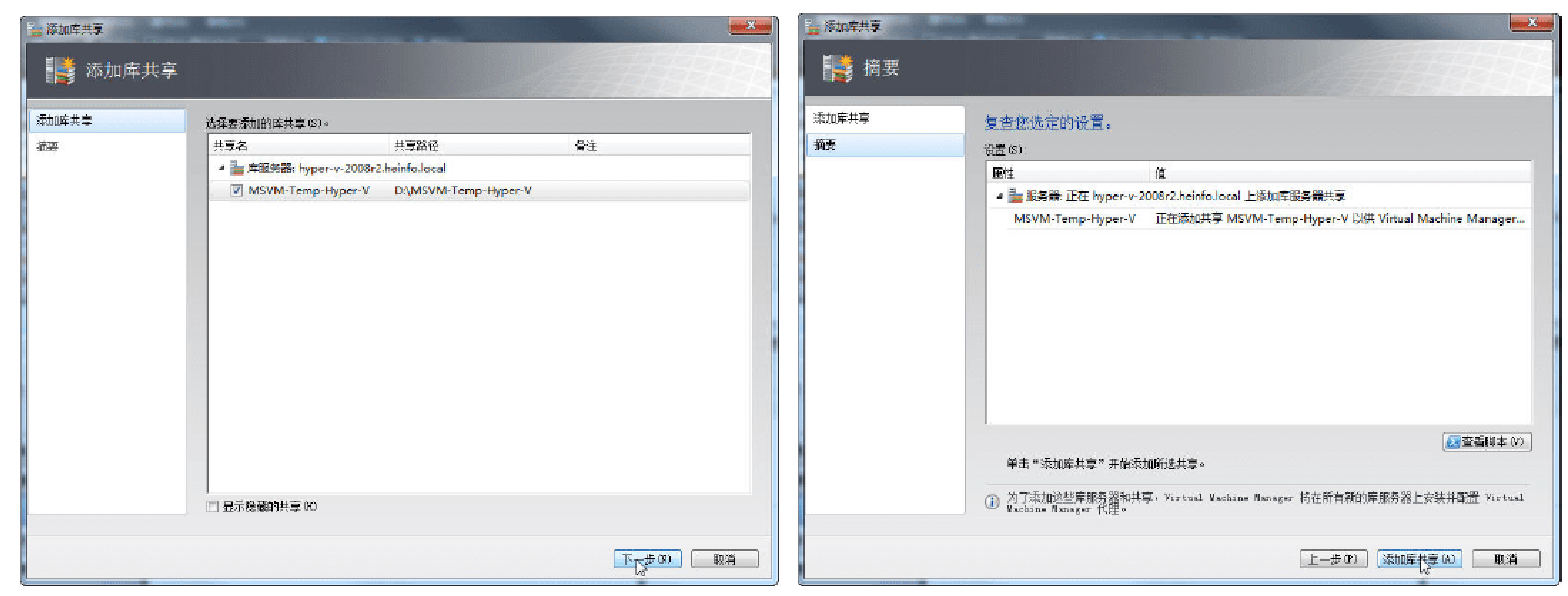


图 12-84　添加库共享　　　　图 12-85　摘要

添加完成之后，参照步骤 1~3，为另一台 Hyper-V 主机添加库共享，在此不再介绍。

12.4.2　准备模板虚拟机

在将“虚拟机”转换为模板之前，还需要对虚拟机进行一系列的定制。在本节中，以前文创建的 Windows Server 2003 虚拟机为例进行介绍。

01 在 Windows Server 2003 虚拟机安装好“虚拟来宾服务”之后，启动并连接到该虚拟机，如图 12-86 所示。

02 在 Windows Server 2003 虚拟机中，启用“交互式登录：不需要按 CTRL+ALT+DEL”属性，如图 12-87 所示。

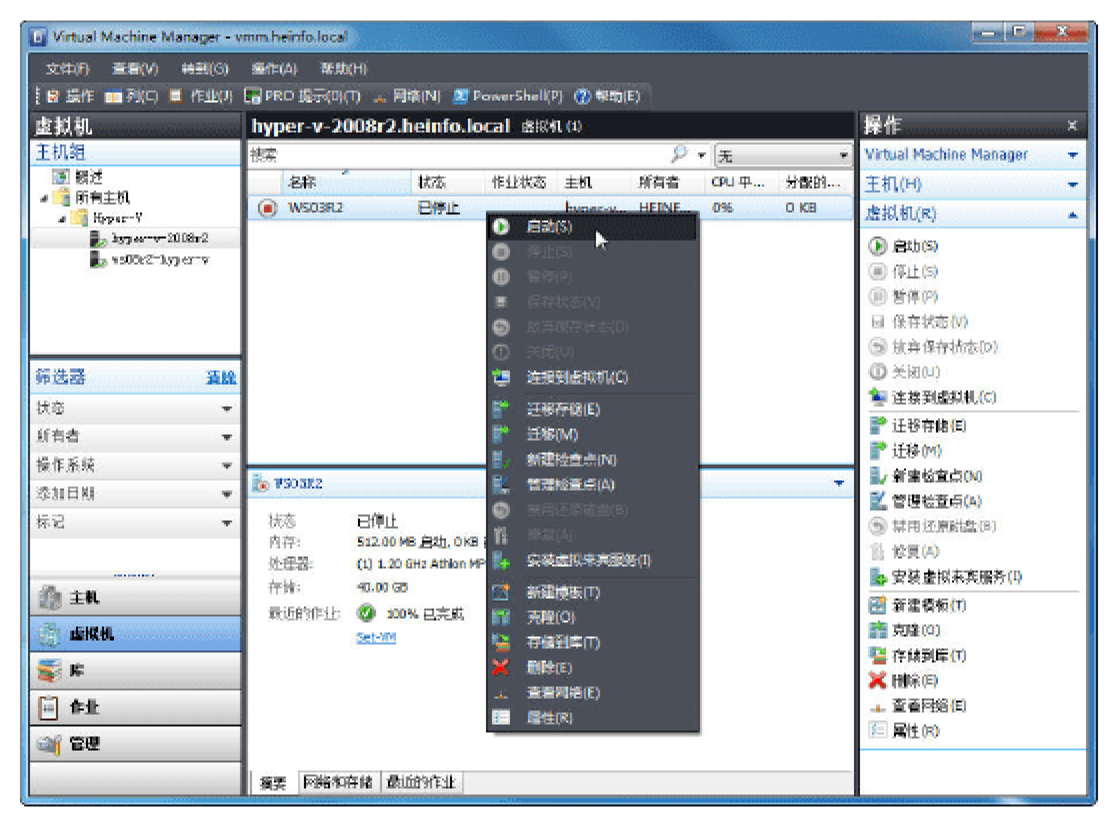


图 12-86 启动虚拟机

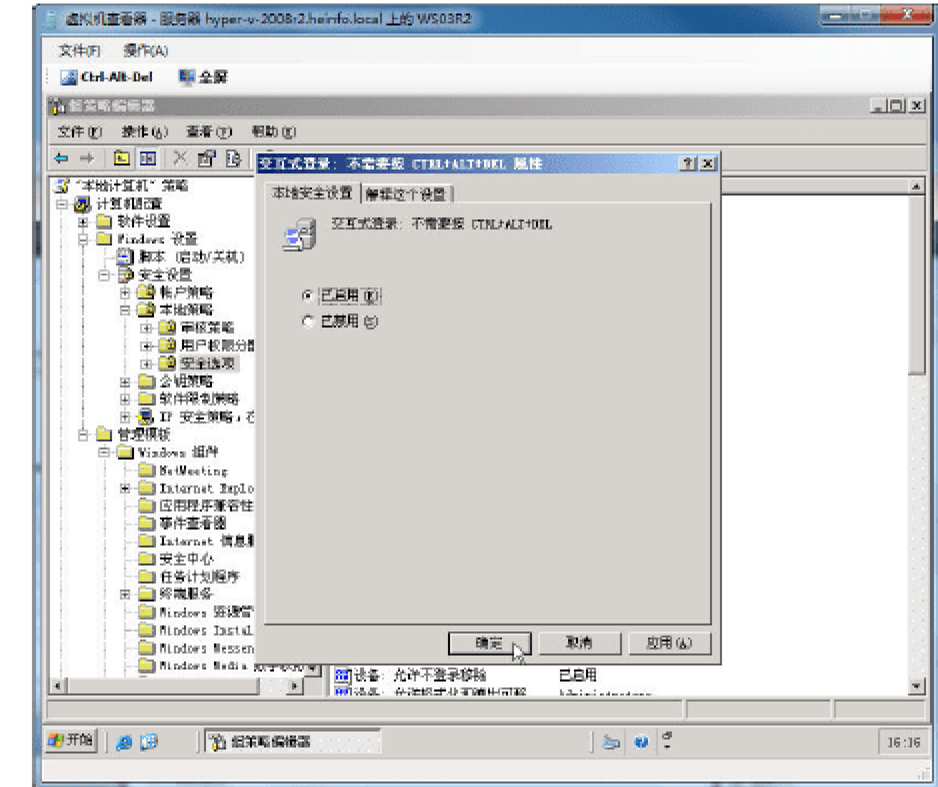


图 12-87 不需要按 CTRL+ALT+DEL 即可登录

03 禁用“显示‘关闭事件跟踪程序’”属性（如图 12-88 所示）以及“激活‘关闭事件跟踪程序系统状态数据’功能”属性，如图 12-89 所示。

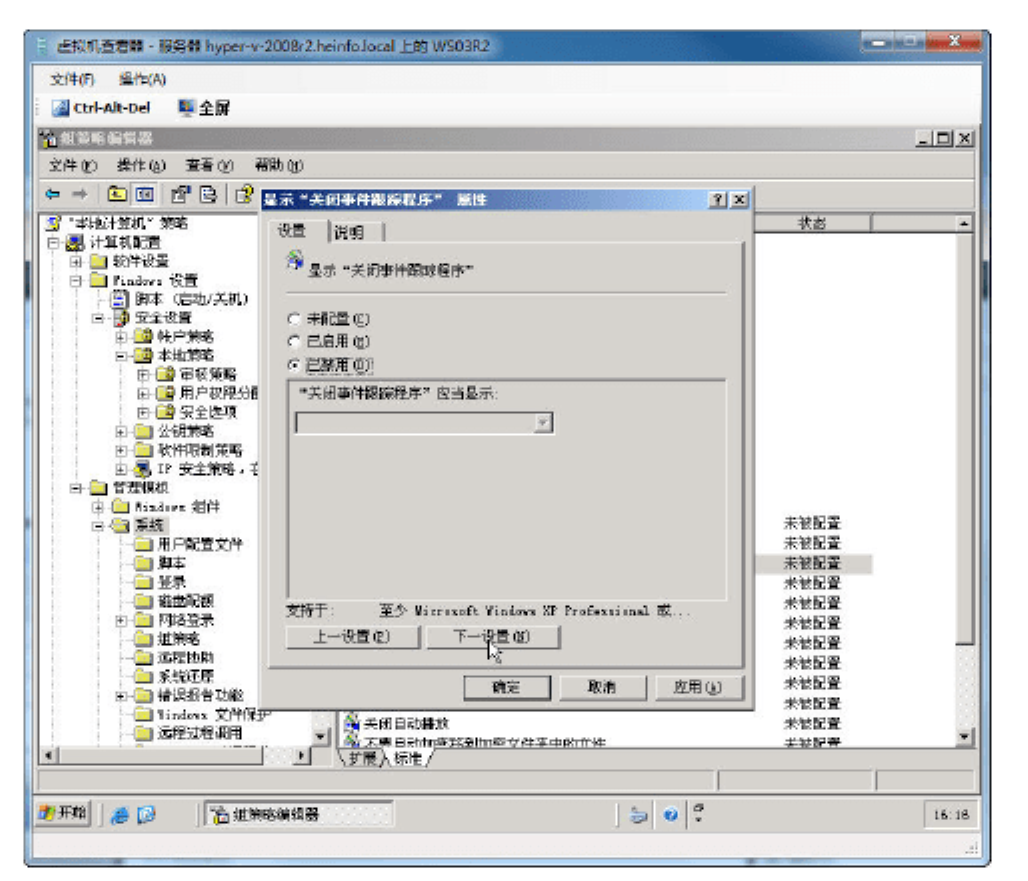


图 12-88 关闭事件跟踪程序

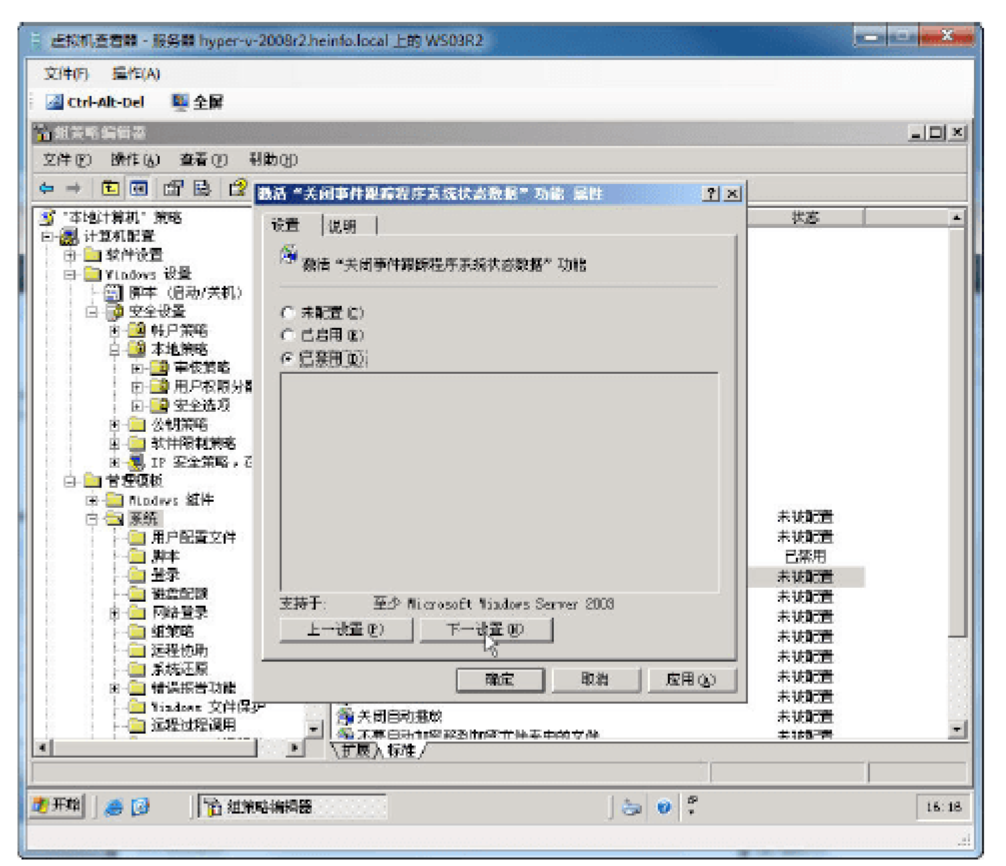


图 12-89 关闭事件跟踪程序状态数据

04 在“控制面板→添加/删除程序”中，确认“Hyper-V 集成服务”已经安装，如图 12-90 所示。

05 修改虚拟机属性，加载 Windows Server 2003 的第 1 张安装光盘，如图 12-91 所示。

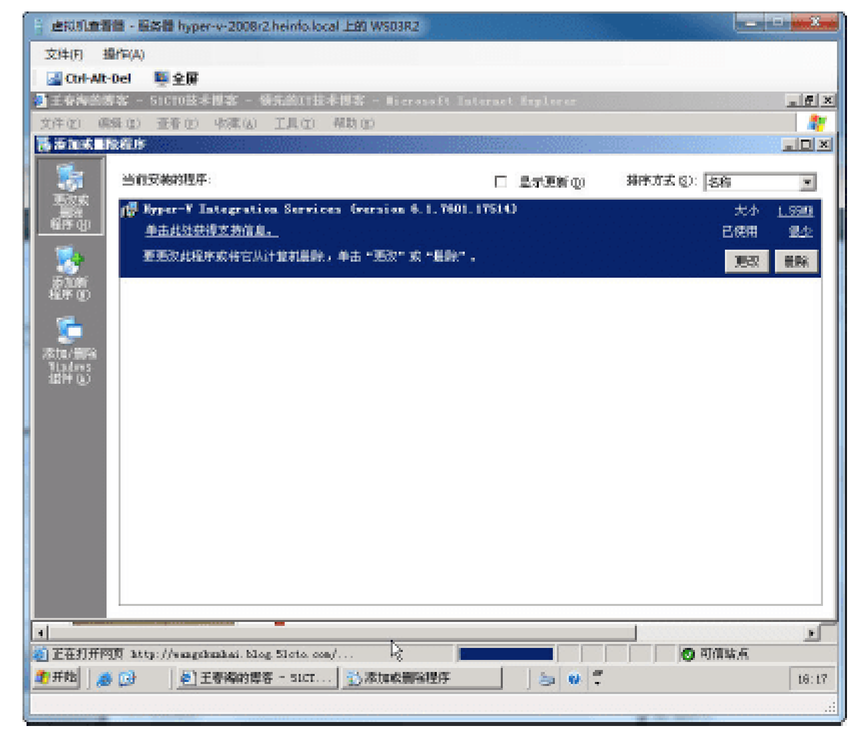


图 12-90 确认集成服务已安装

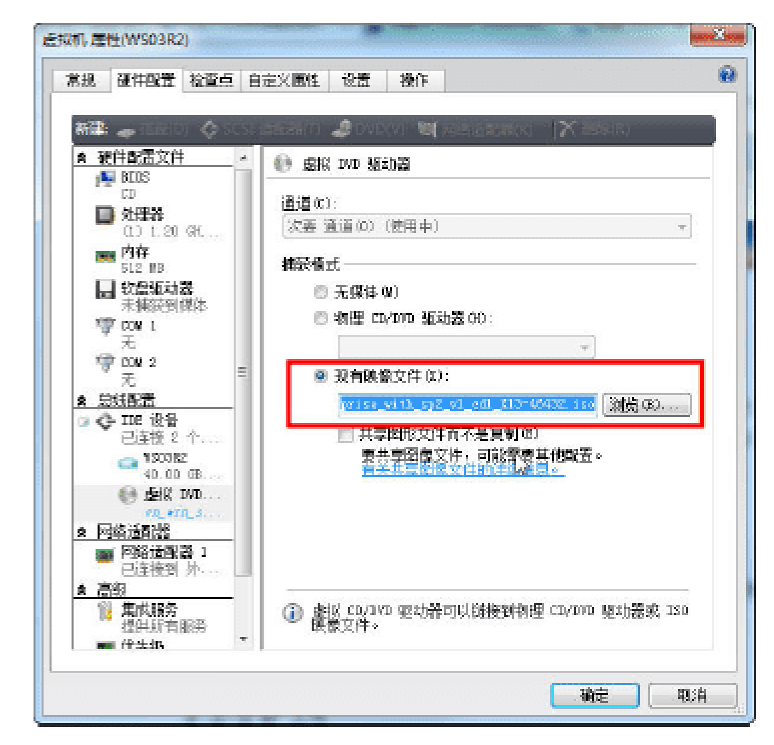


图 12-91 加载 Windows Server 2003 安装光盘

06 进入 Windows Server 2003 虚拟机，在 Windows Server 2003 安装光盘的\SUPPORT\TOOLS 目录中，从 DEPLOY.CAB 中“提取”所有文件，如图 12-92 所示。

07 将 DEPLOY.CAB 中所有文件提取到 C 盘 sysprep 文件夹中（选中 C 盘单击“新建文件夹”，创建这个文件夹），如图 12-93 所示。

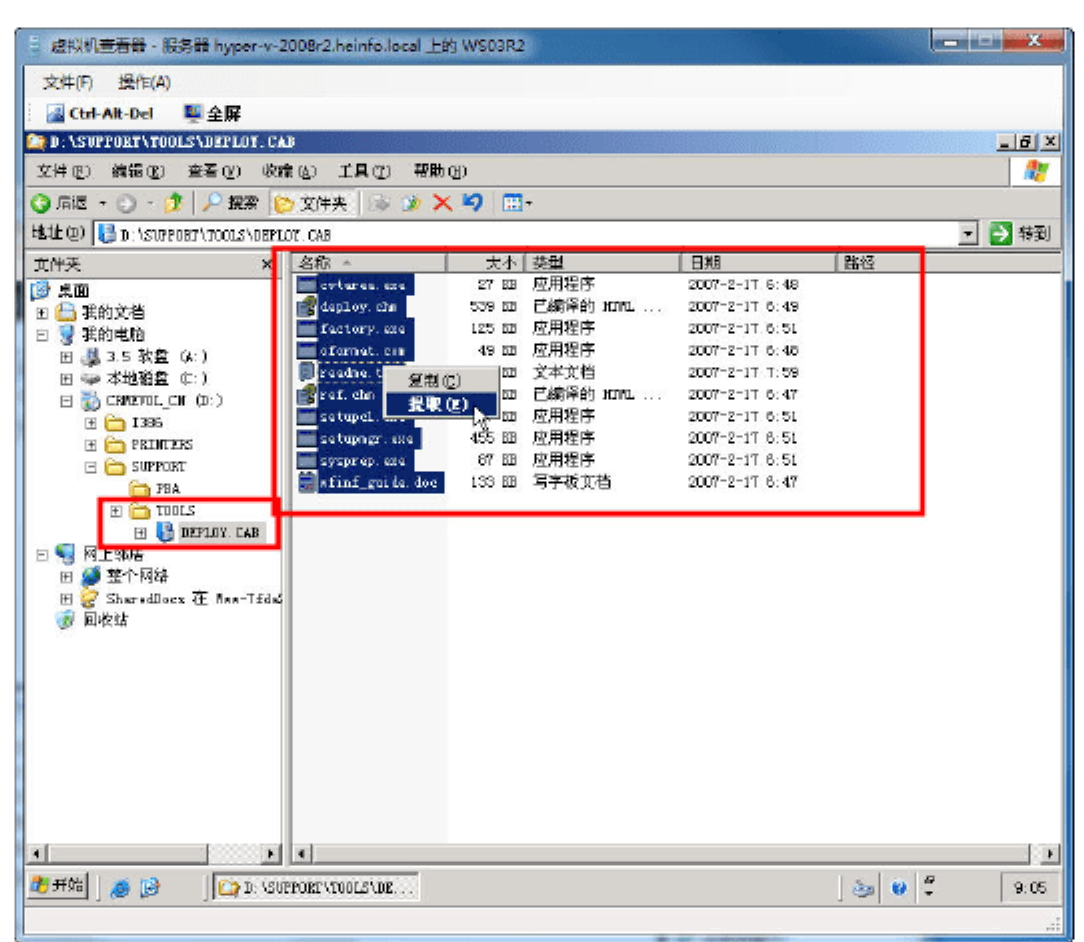


图 12-92　提取文件 1

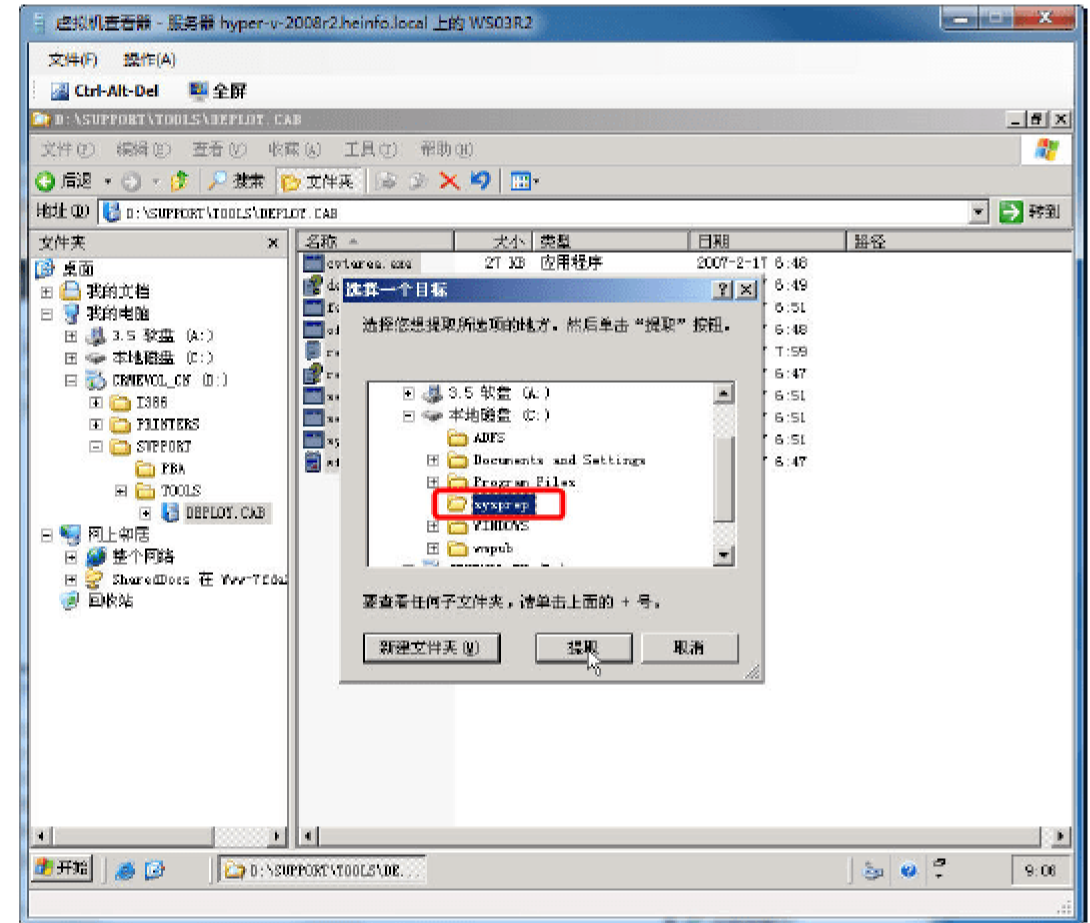


图 12-93　提取文件 2

08 然后定位到 C:\sysprep 文件夹，运行 setupmgr.exe（如图 12-94 所示），进入“安装管理器”对话框，如图 12-95 所示，单击“下一步”按钮。

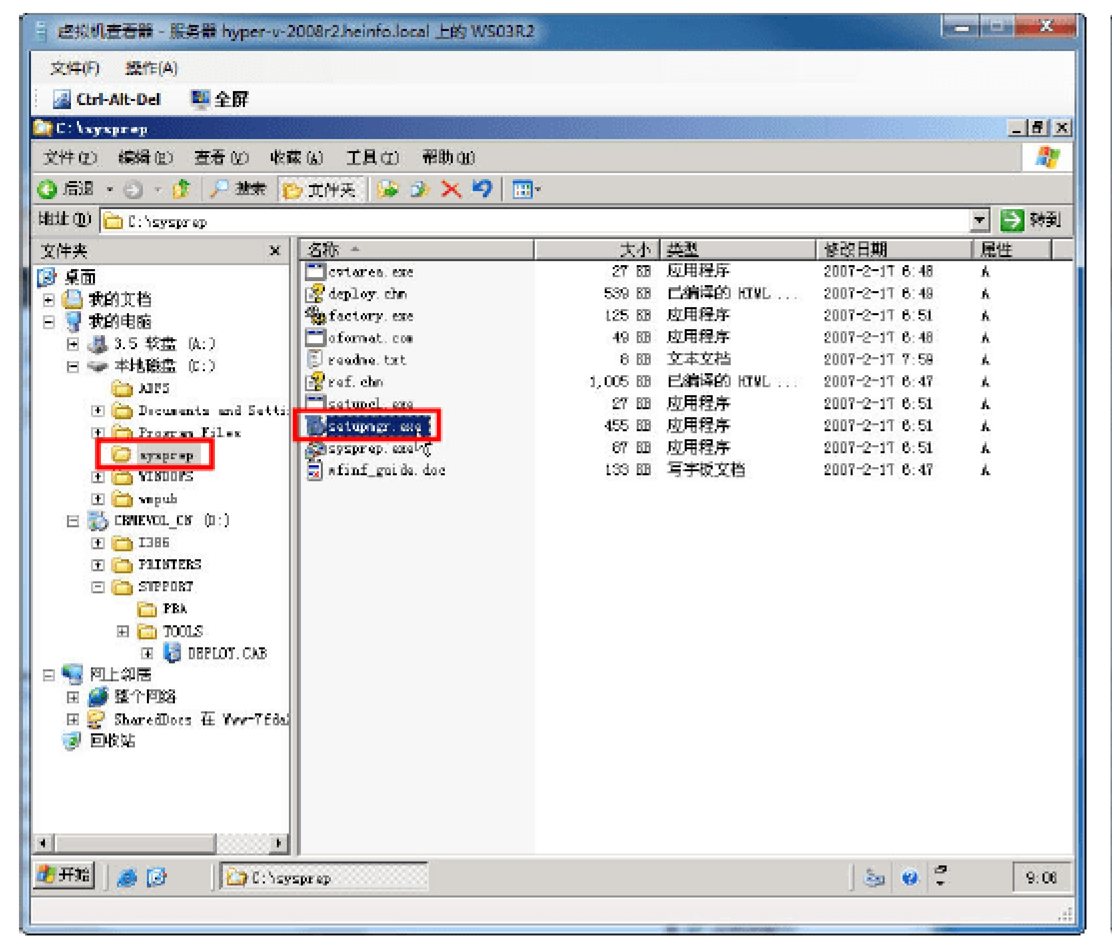


图 12-94　setupmgr.exe 程序

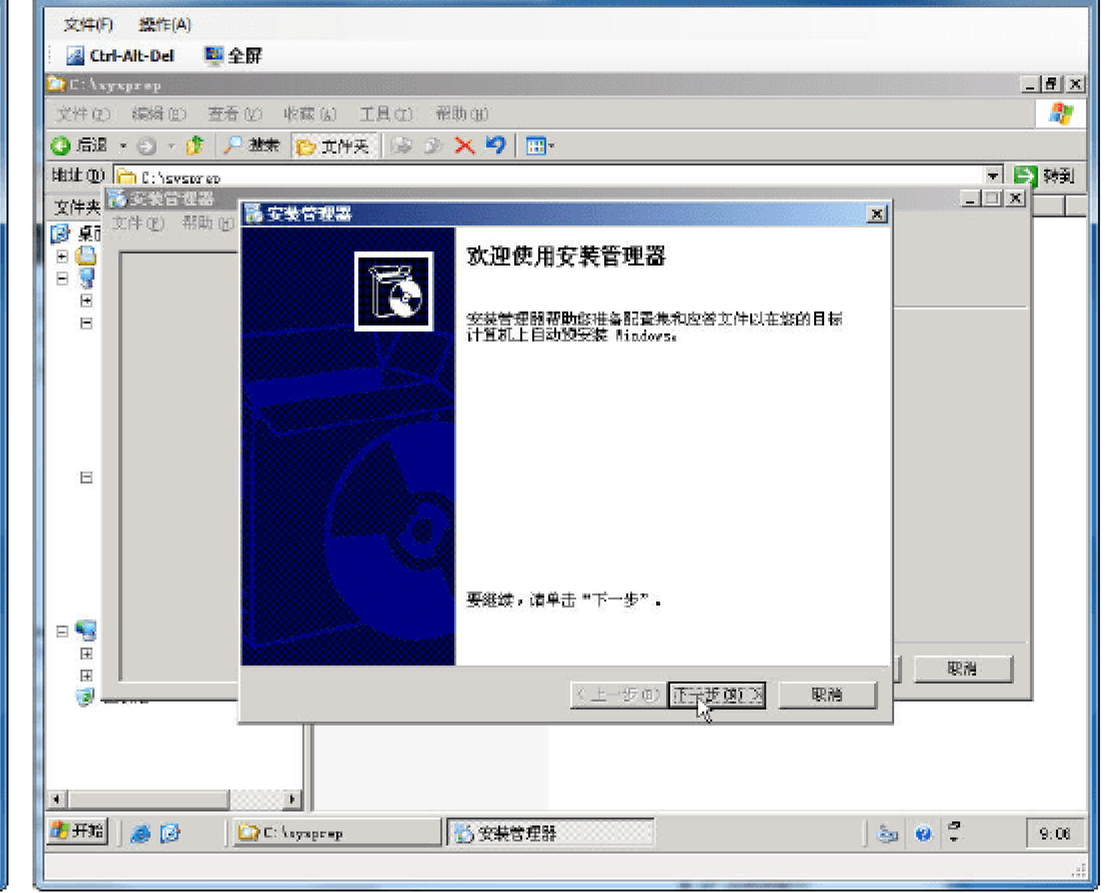


图 12-95　安装管理器

09 进入“新的或现有的应答文件”对话框中，选择“创建新文件”单选按钮，如图 12-96 所示。

10 在“安装的类型”对话框中选中“Sysprep 安装”单选按钮，如图 12-97 所示。

11 在“产品”对话框中，选择该应答文件用于的 Windows 产品，在此选择 Windows Server 2003 企业版，如图 12-98 所示。

12 在“许可协议”对话框中，选中“是，完全自动安装”单选按钮，如图 12-99 所示。

图 12-96　创建新文件

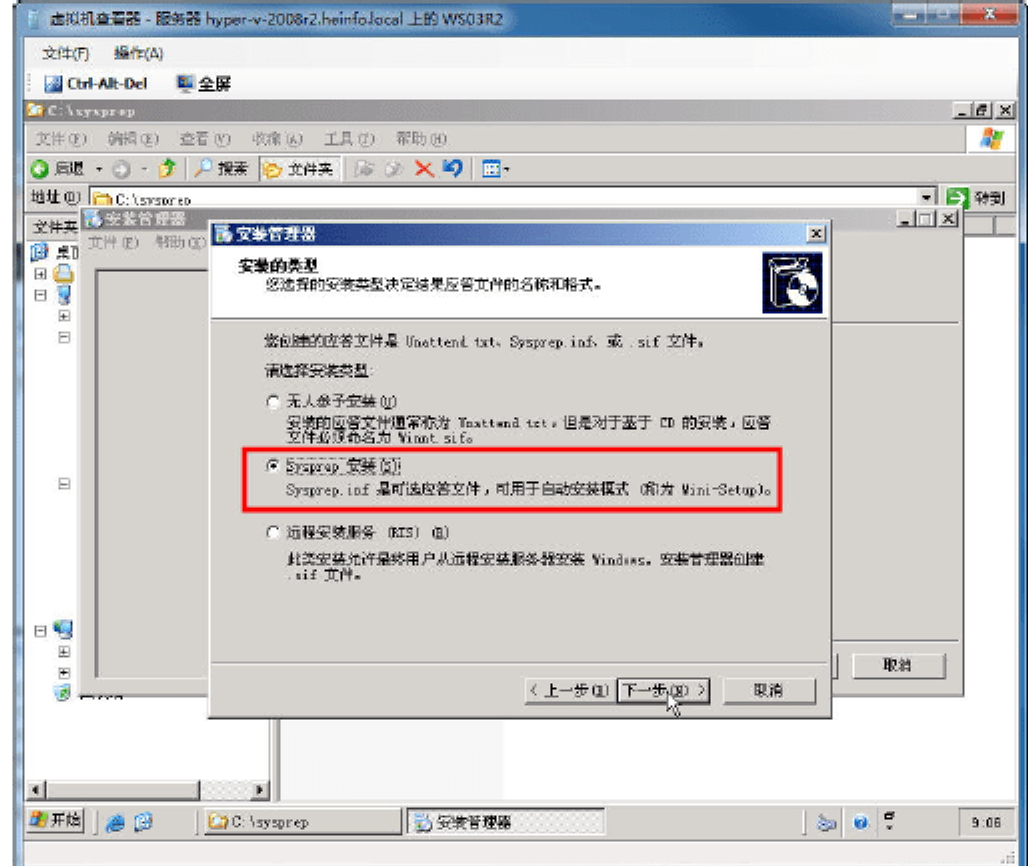


图 12-97　选择安装类型

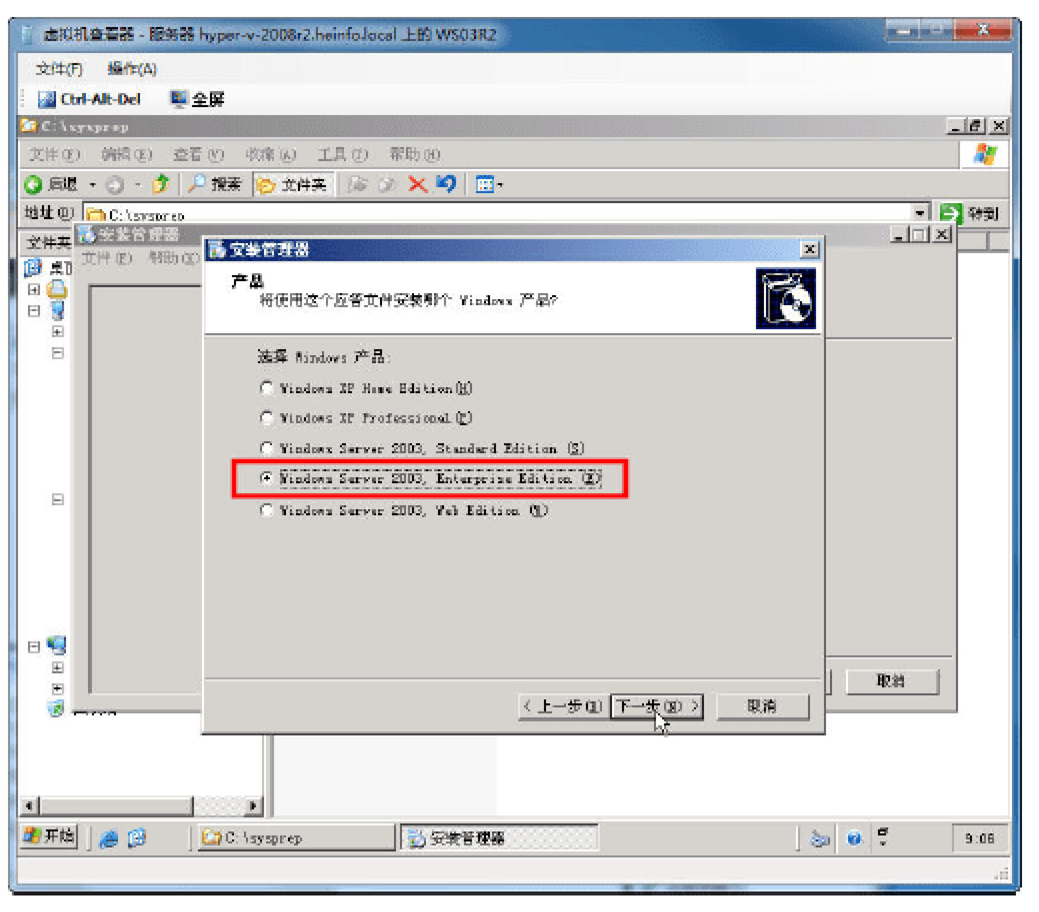


图 12-98　选择应答文件使用的产品

图 12-99　许可协议

13 在“时区”对话框中，选择北京时间，如图 12-100 所示。

14 在“产品密钥”对话框中，输入 Windows Server 2003 企业版的安装序列号，如图 12-101 所示。

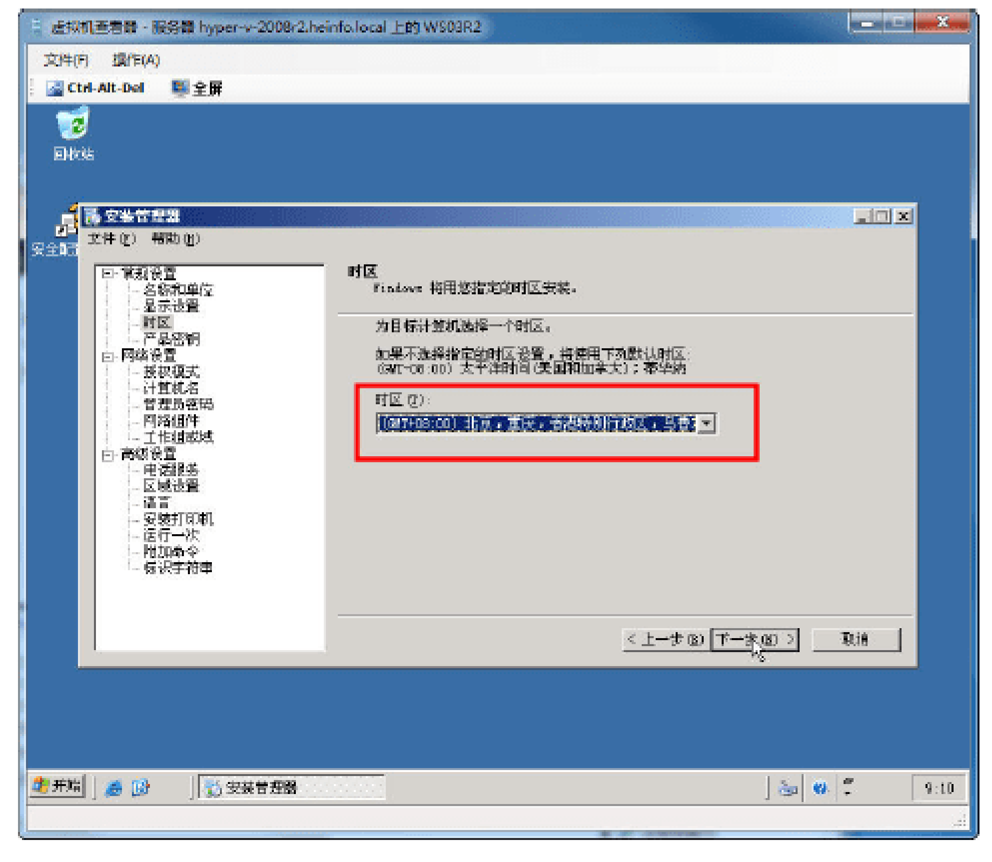


图 12-100　选择时区

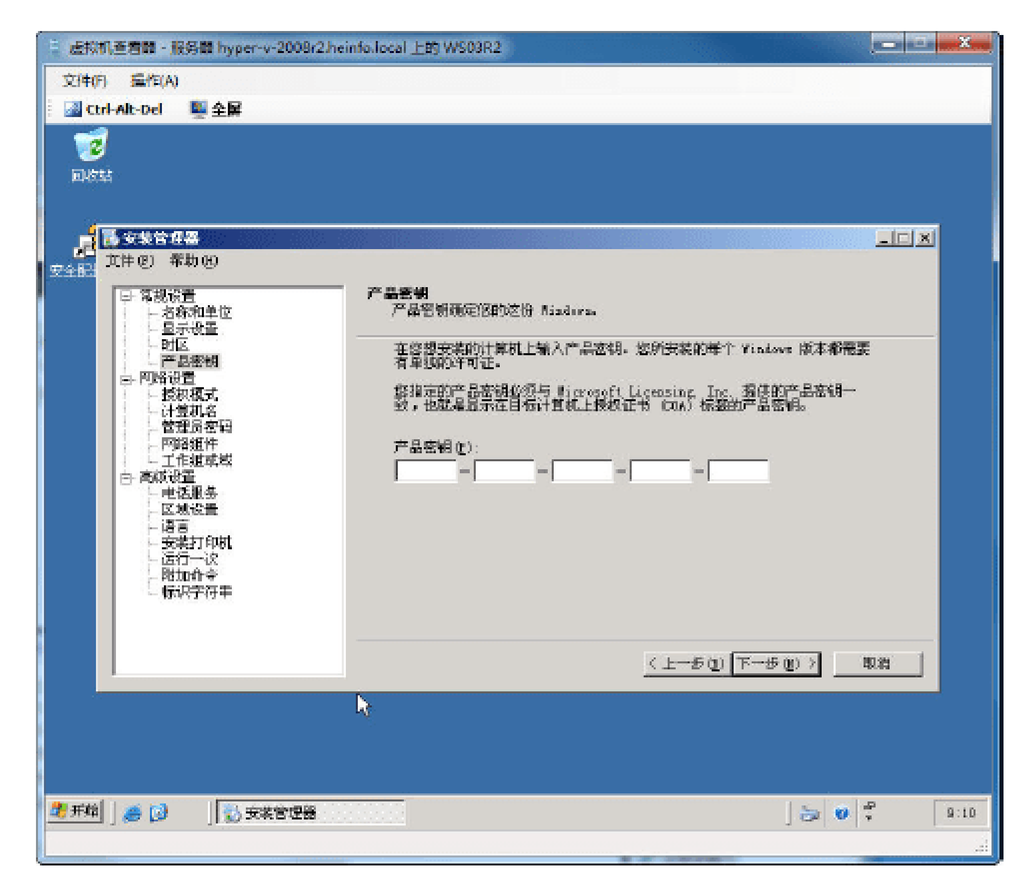


图 12-101　输入产品密钥

15 在“计算机名”对话框中，选中“自动产生计算机名”单选按钮，如图 12-102 所示。

16 在“管理员密码”对话框中，设置 Administrator 密码，并且可以选择让 Administrator 自动登录的次数，如图 12-103 所示。

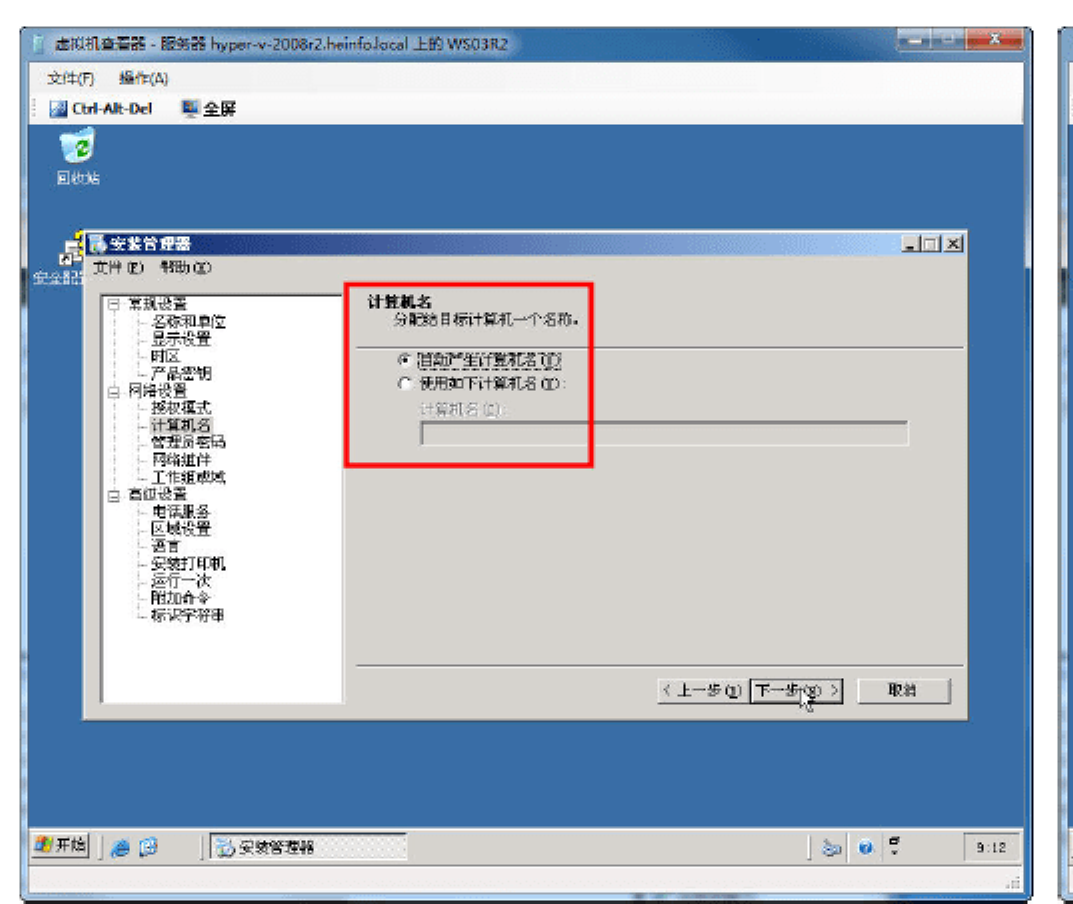


图 12-102　自动产生计算机名

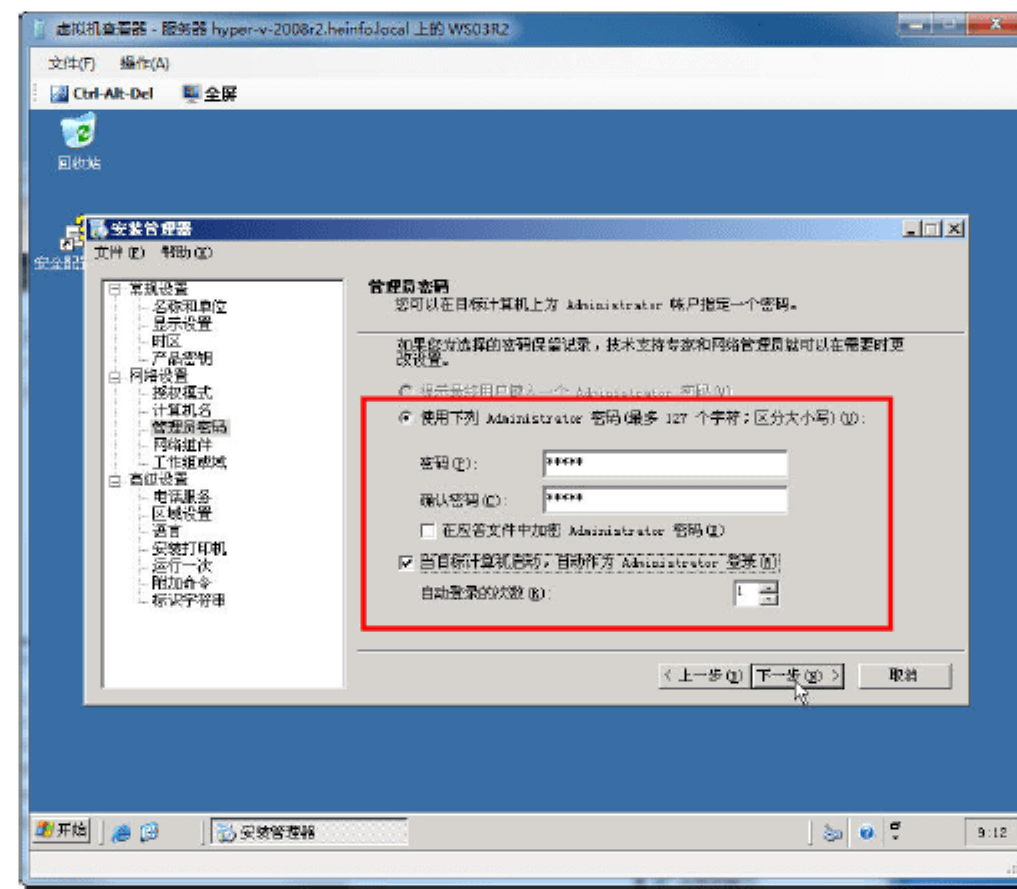


图 12-103　管理员密码

17 在“工作组或域”对话框中，设置计算机是加入到域，还是加入到工作组，如图 12-104 所示。如果要加入到域，还需要指定域名与具有“将计算机加入到域”的权限的域用户，以及对应的域用户密码。

18 在“标识字符串”对话框中，设置该 sysprep 配置文件的标识信息，然后将其保存在 C:\sysprep 文件夹，保存文件名为 sysprep.inf，如图 12-105 所示。

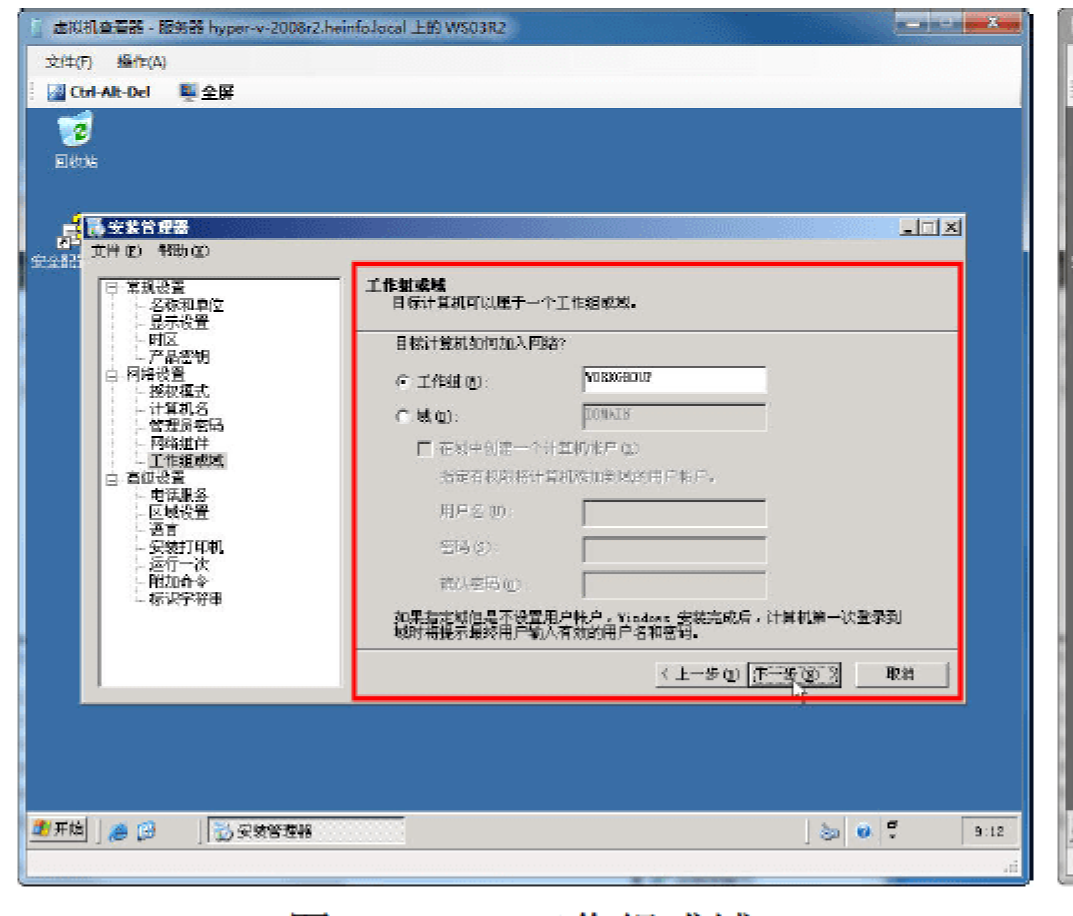


图 12-104　工作组或域

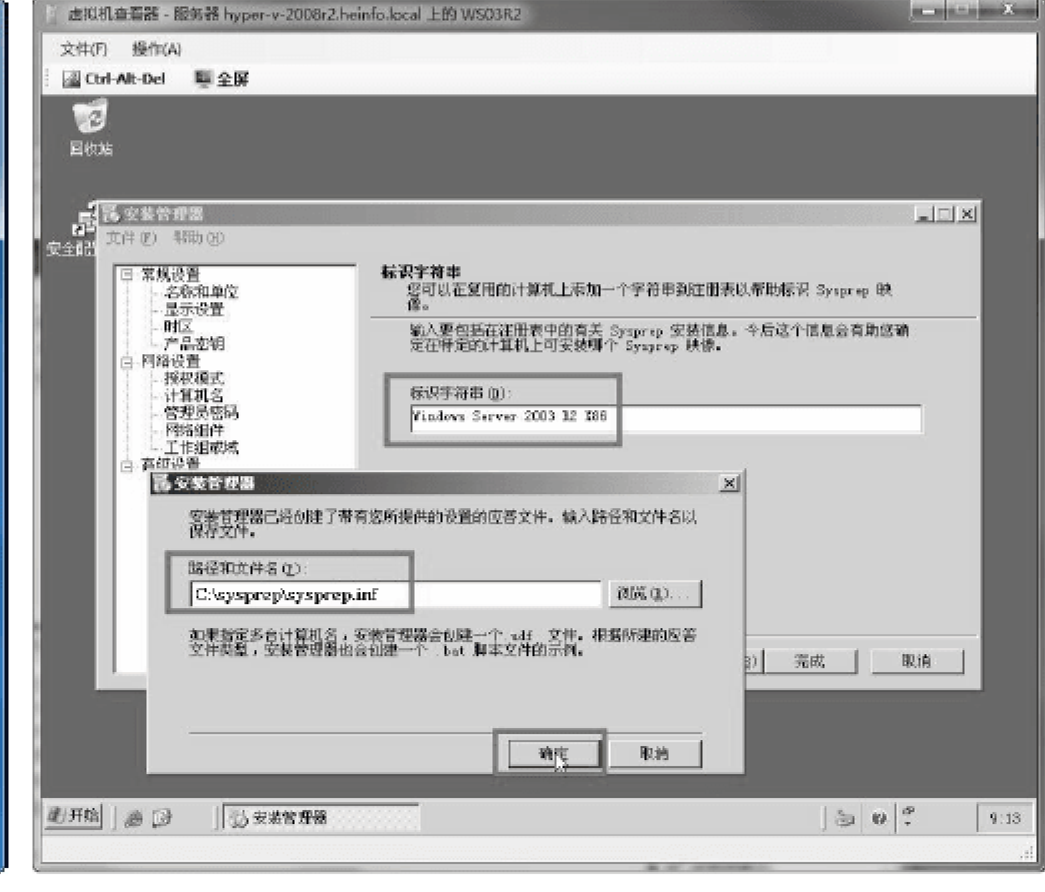


图 12-105　保存配置文件名

19 配置管理器运行完成后，进入命令提示窗口，在 C:\sysprep 文件夹中执行 sysprep 程序，并在“系统准备工具 2.0”对话框中，在“关机模式”下拉列表中选择“关机”选项，单击“重新封装”按钮，在弹出的对话框中单击“确定”按钮，如图 12-106 所示。

20 运行系统准备工具之后，Windows Server 2003 自动关机，如图 12-107 所示。

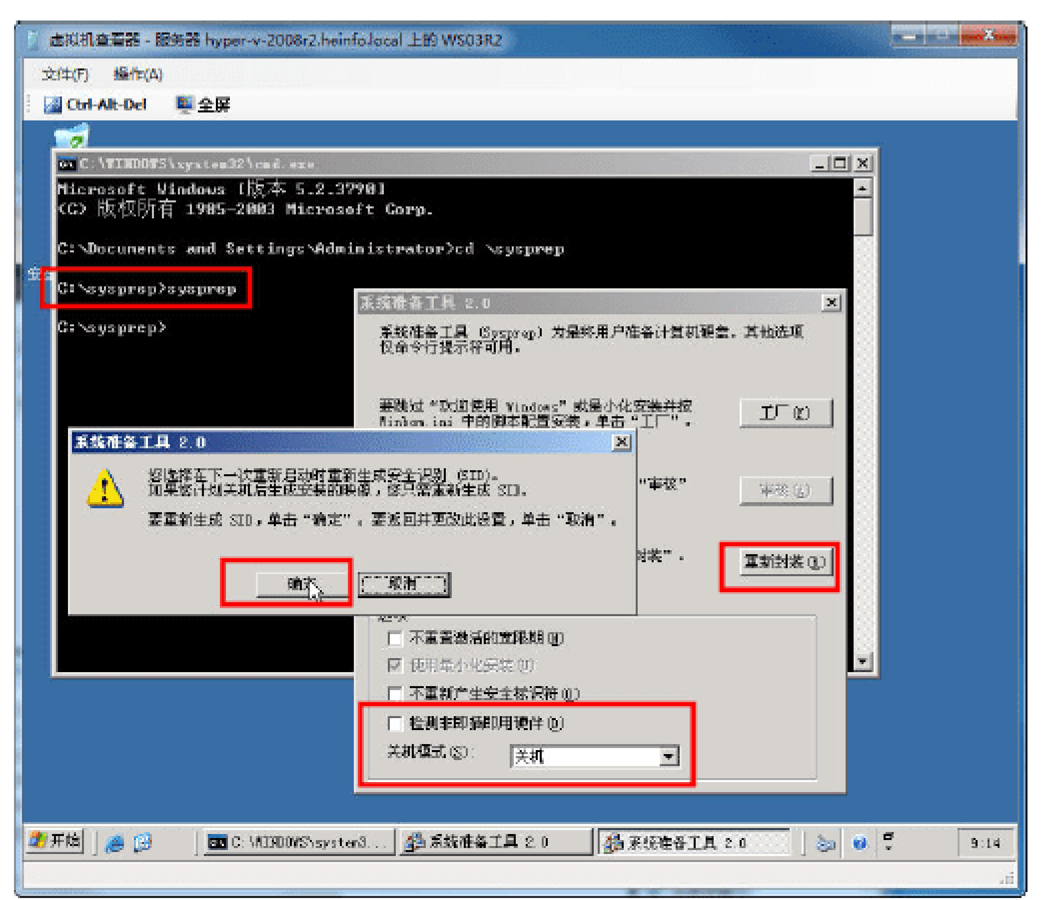


图 12-106 运行系统准备工具

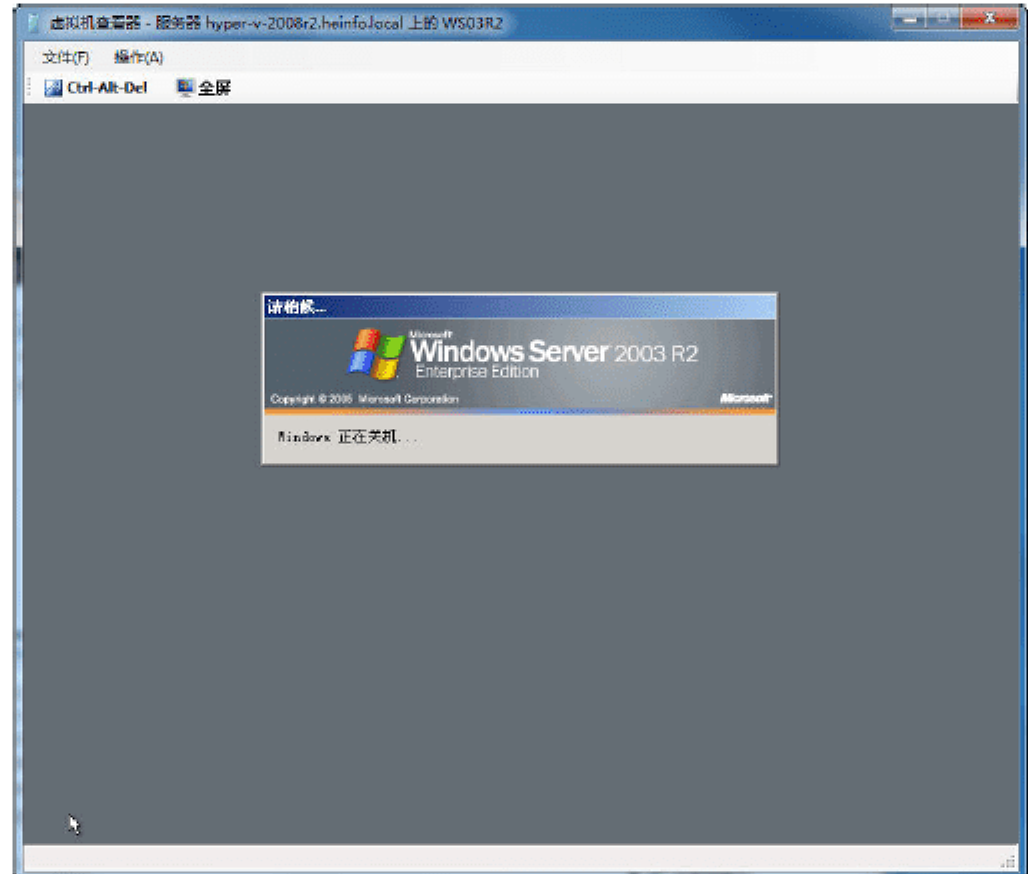


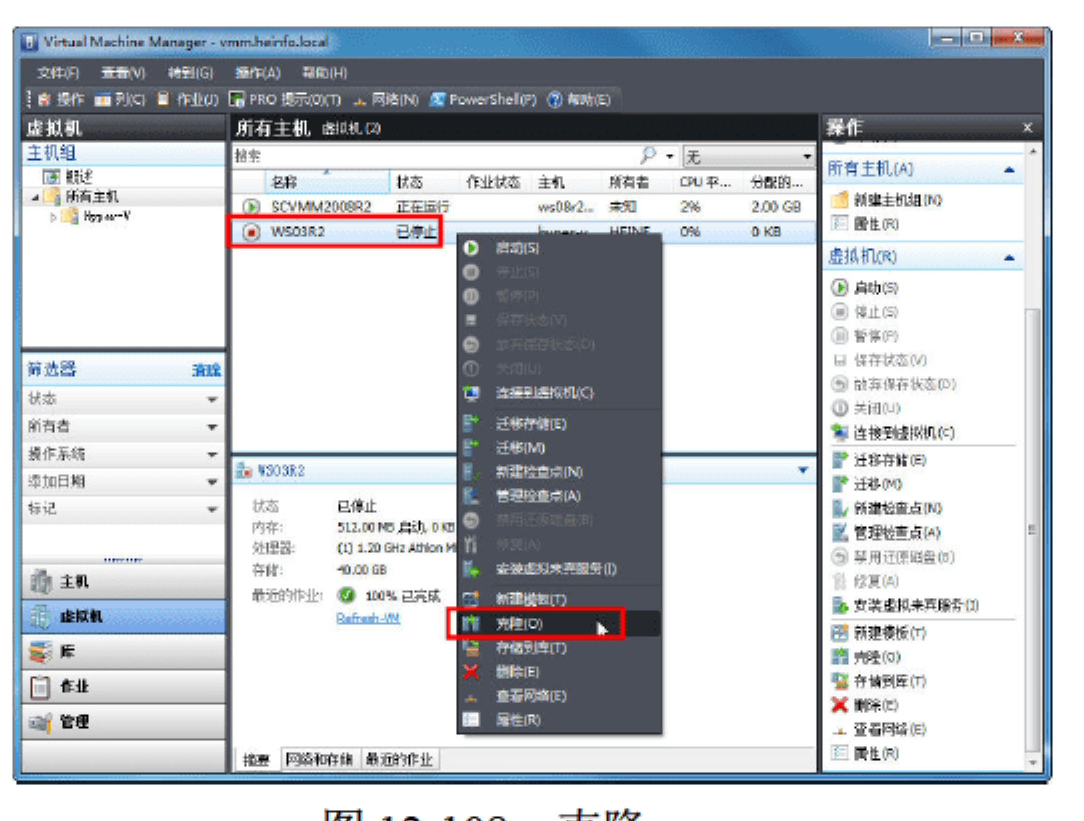
图 12-107 运行系统准备工具之后关机

12.4.3 克隆虚拟机

在将虚拟机转换为模板的时候，会破解源虚拟机的数据。所以，在转换之前，通常要将源虚拟机创建一个新的克隆，使用新的克隆虚拟机，转换为模板。创建克隆虚拟机的步骤如下。

01 用鼠标右击已经关闭的虚拟机，在弹出的快捷菜单中选择“克隆”命令，如图 12-108 所示。

02 在“虚拟机标识”对话框中，设置新的虚拟机的名称。在本例中，指定为 WS03R2-Temp，如图 12-109 所示。



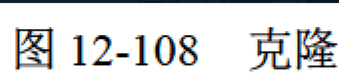


图 12-108 克隆

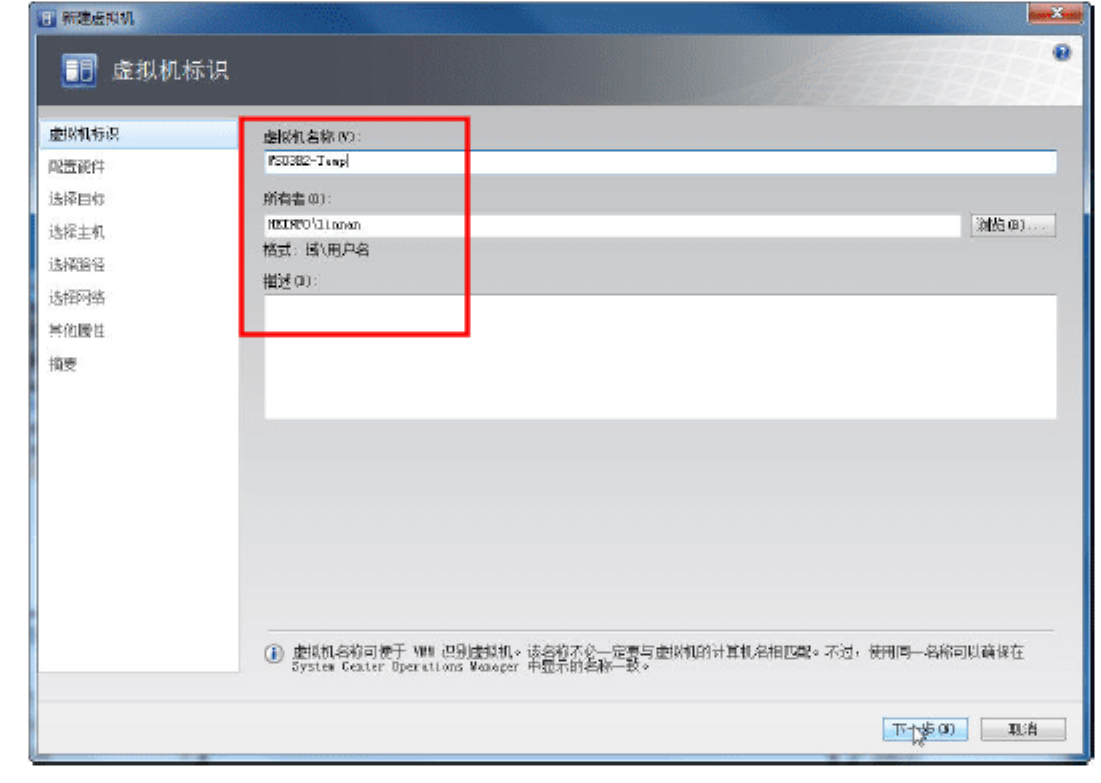


图 12-109 虚拟机标识

03 在“配置硬件”对话框中，设置新克隆的虚拟机的内存、CPU、硬盘等信息，如图 12-110 所示。可以根据实际情况进行相关的设置，或者使用默认值。

04 在“选择目标”对话框中，选中要部署虚拟机还是存储虚拟机，选择“将虚拟机放置到主机上”单选按钮，如图 12-111 所示。



图 12-110　配置硬件　　　　　　图 12-111　选择目标

05 在“选择主机”对话框中，为虚拟机选择主机，如图 12-112 所示。

06 在“选择路径”对话框中，选择虚拟机文件在主机上的存储位置，如图 12-113 所示。

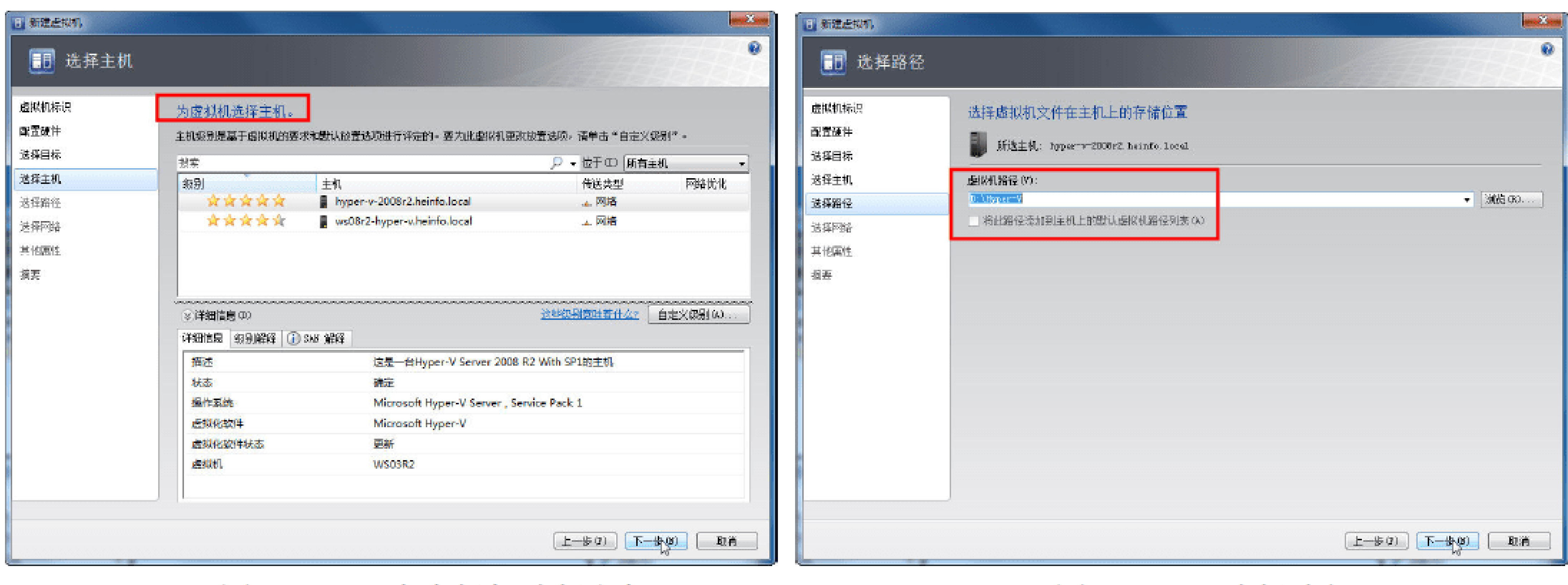


图 12-112　为虚拟机选择主机　　　　　　图 12-113　选择路径

07 在“选择网络”对话框中，指定用于虚拟机的虚拟网络。

08 在“其他属性”对话框中，指定自动启动操作、操作系统等选项，这些都选择默认值即可。

09 在“摘要”对话框中，显示克隆的虚拟机的相关信息，设置无误之后，单击“创建”按钮，如图 12-114 所示。注意，不要选中“在主机上部署虚拟机之后启动虚拟机”复选框。

10 在创建虚拟机的“作业”窗口，在“详细信息”中可以看到有一项“修复差异磁盘”的状态是 0%，对于当前这个操作来说这是正常的。当“创建虚拟机”的“状态”是“已完成”时，单击“取消作业”按钮即可，如图 12-115 所示。

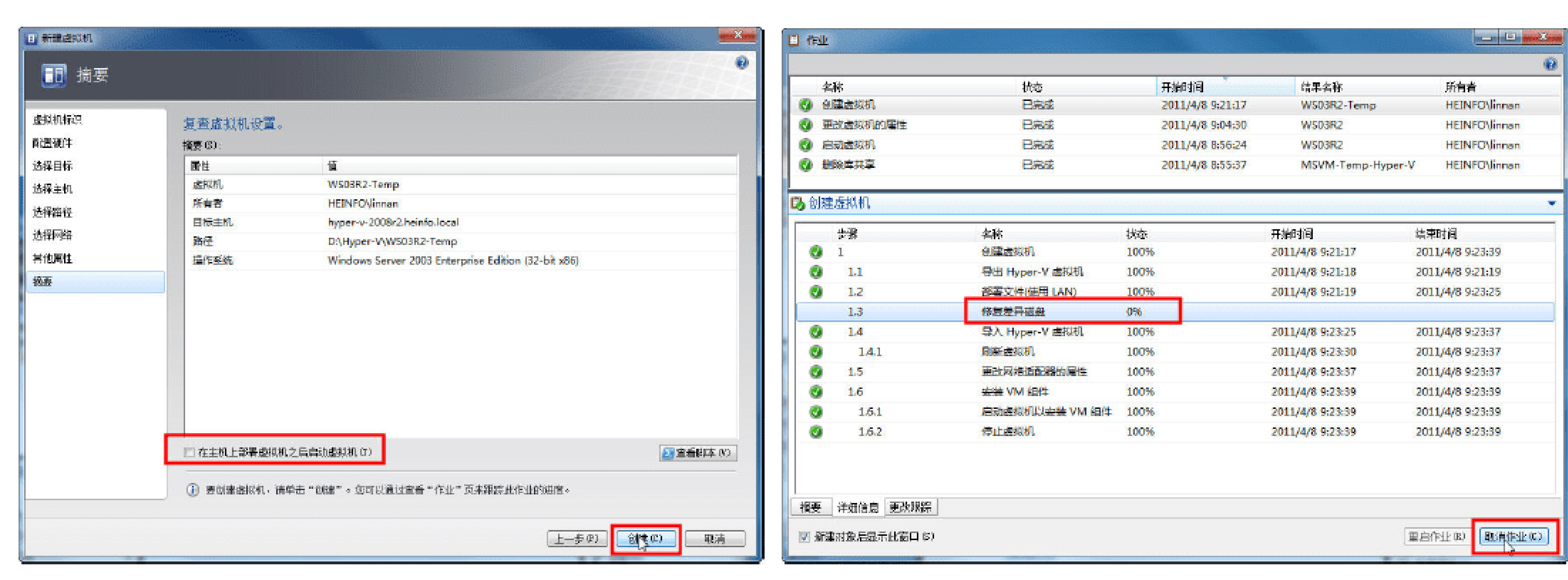


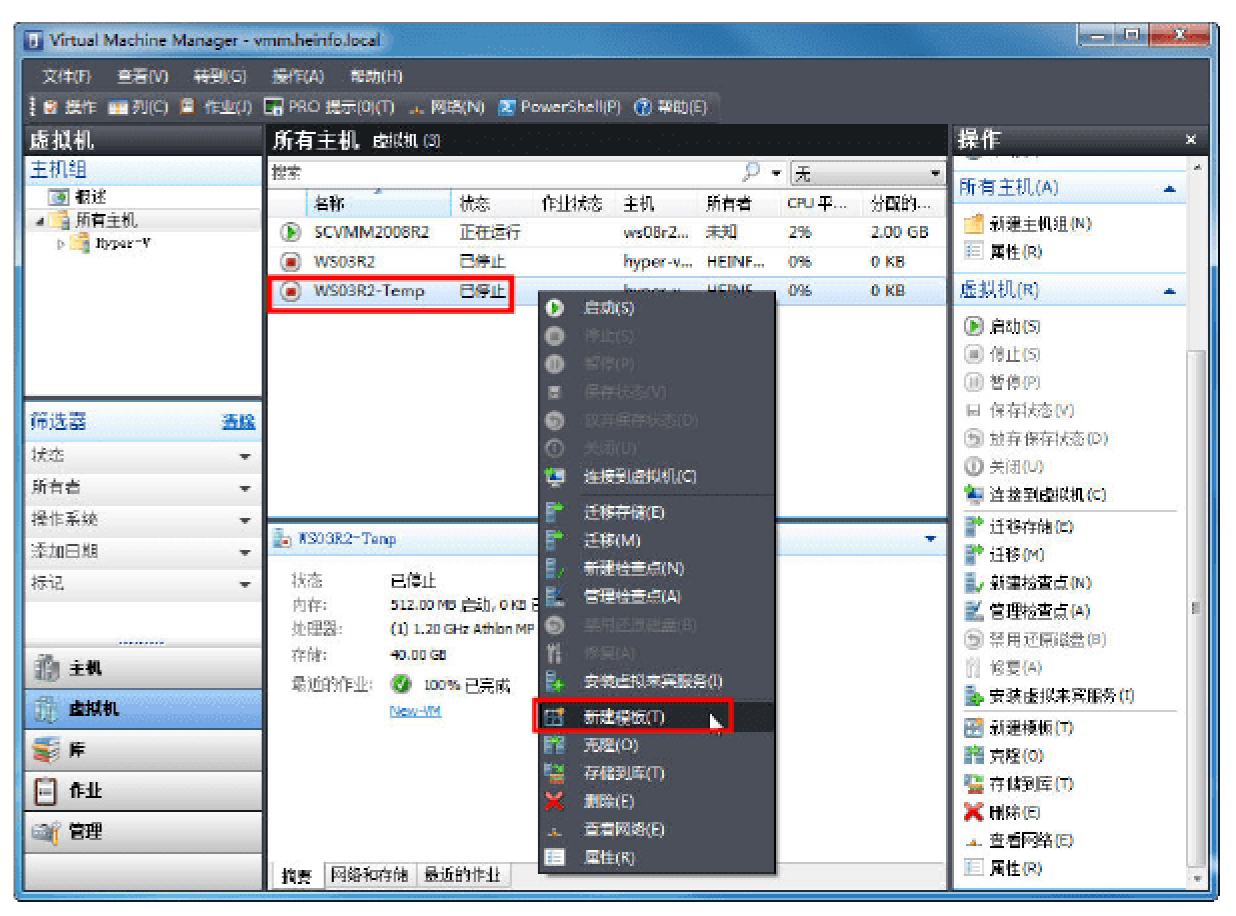
图 12-114　创建虚拟机　　　　图 12-115　创建完成

12.4.4　将克隆虚拟机转换为模板

在创建好克隆虚拟机之后，接下来就可以将克隆的虚拟机转换为模板，步骤如下。

01 在 VMM 管理员控制台中，右击新克隆的 Windows Server 2003 虚拟机，在弹出的快捷菜单中选择“新建模板”命令，如图 12-116 所示。

02 在弹出的警告信息中单击“是”按钮，如图 12-117 所示。



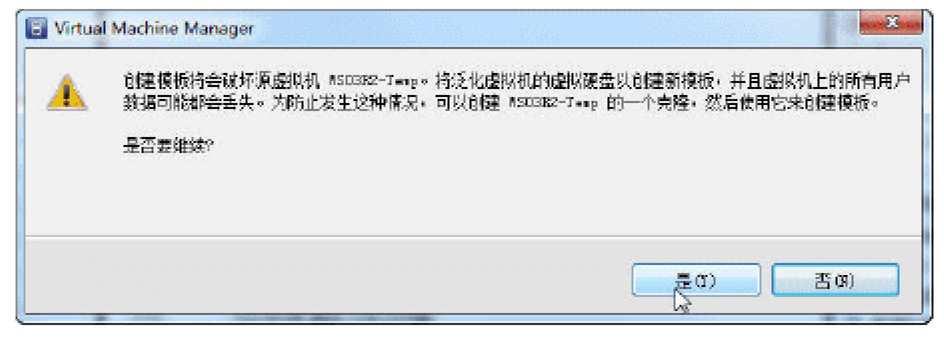


图 12-116　新建模板　　　　图 12-117　警告信息

03 在“模板标识”对话框中，设置虚拟机的模板名称，默认与要转换的虚拟机同名，如图 12-118 所示。

04 在“配置硬件”对话框中，保持默认值，如图 12-119 所示。

05 在“来宾操作系统”对话框中，指定管理员密码、标识信息、产品密钥等，如图 12-120 所示。

06 在“选择库服务器”对话框中，选择保存模板虚拟机的主机，在此选择 172.30.5.31 的物理主机（计算机名为 ws08r2-hyper-v.heinfo.local），如图 12-121 所示。

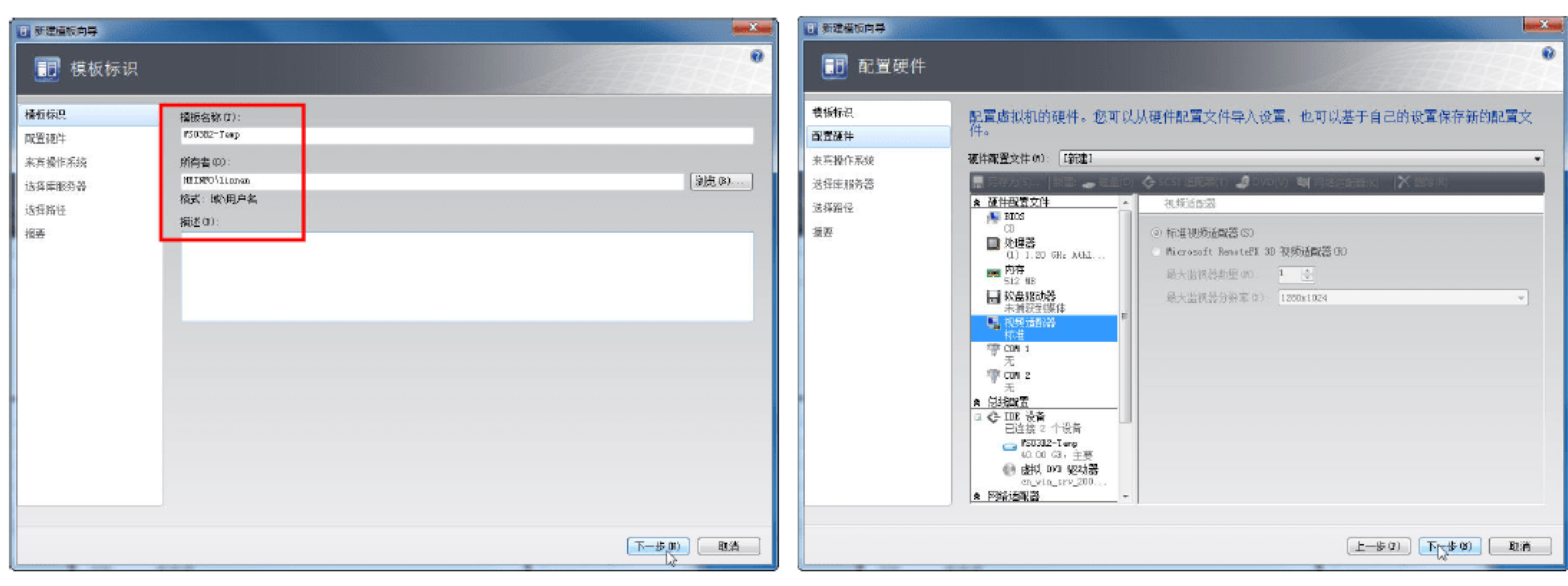


图 12-118 模板标识　　图 12-119 配置硬件

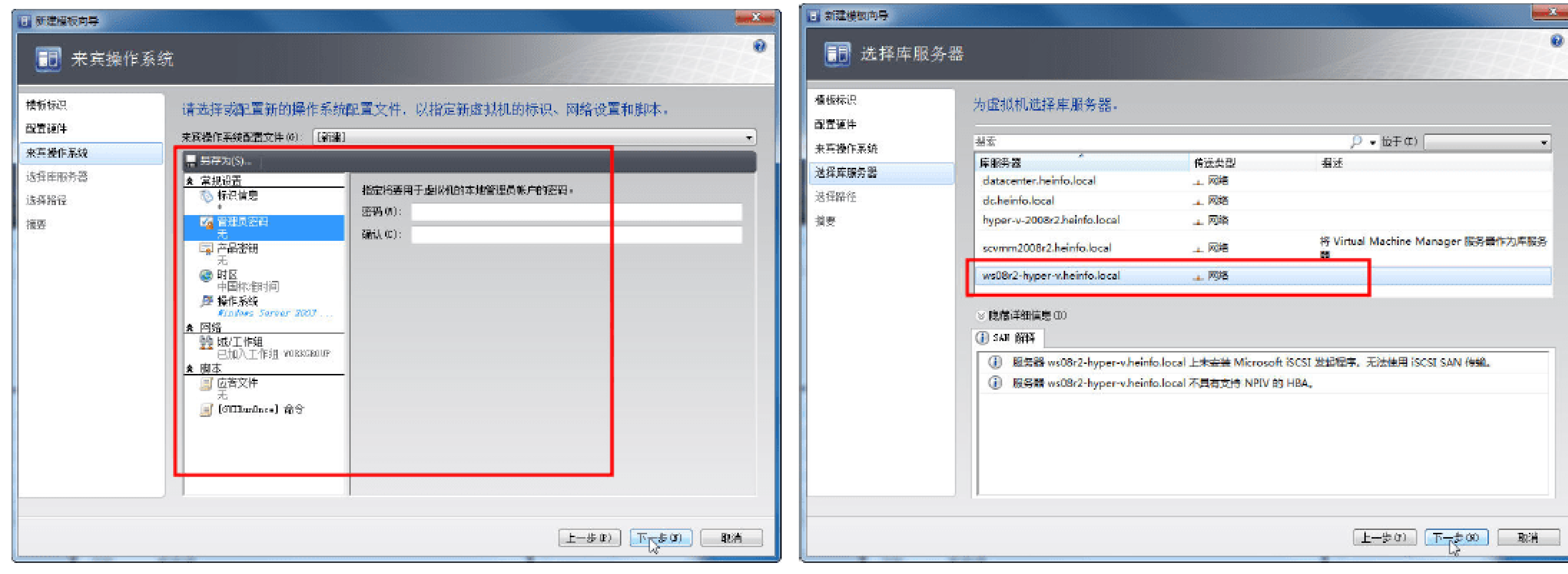


图 12-120 来宾操作系统　　图 12-121 选择库服务器

07 在“浏览目标文件夹”对话框中，选择保存虚拟机的库共享文件夹，在这台库主机上，共享文件夹是 MSVM-Temp，如图 12-122 所示。

08 在“选择路径”对话框中，显示出前面选择的库服务器及库共享文件夹，如图 12-123 所示。

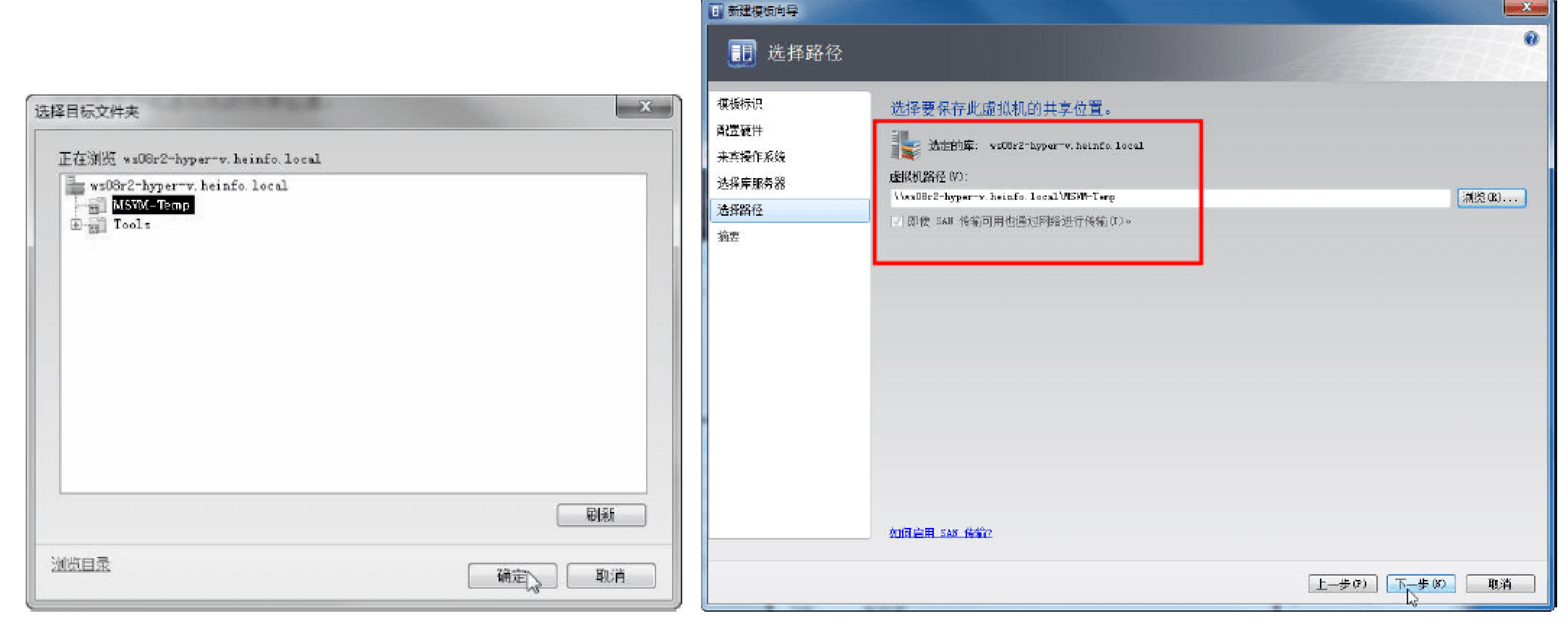


图 12-122 选择库共享文件夹　　图 12-123 选择路径

09 在“摘要”对话框中，显示创建新模板的设置，无误之后单击“创建”按钮，如图 12-124

所示。

10 弹出“作业”窗口，开始创建模板，创建完模板之后，可能会有“返回信息”，单击“取消作业”按钮即可，如图 12-125 所示。

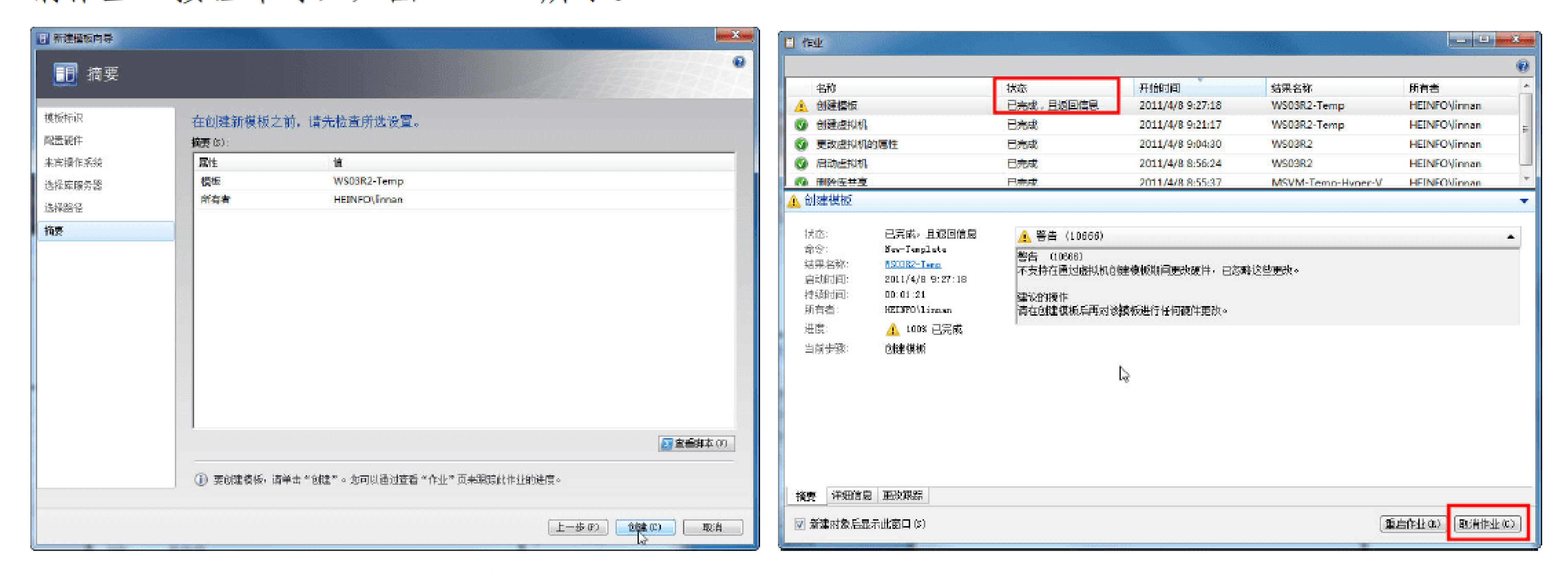


图 12-124　摘要　　　　图 12-125　作业完成

11 转换模板完成之后，在 VMM 管理员控制台中，在“库→资源”列表中，定位到保存模板的库服务器，在库共享文件夹中，可以看到转换后的虚拟机文件夹，如图 12-126 所示。

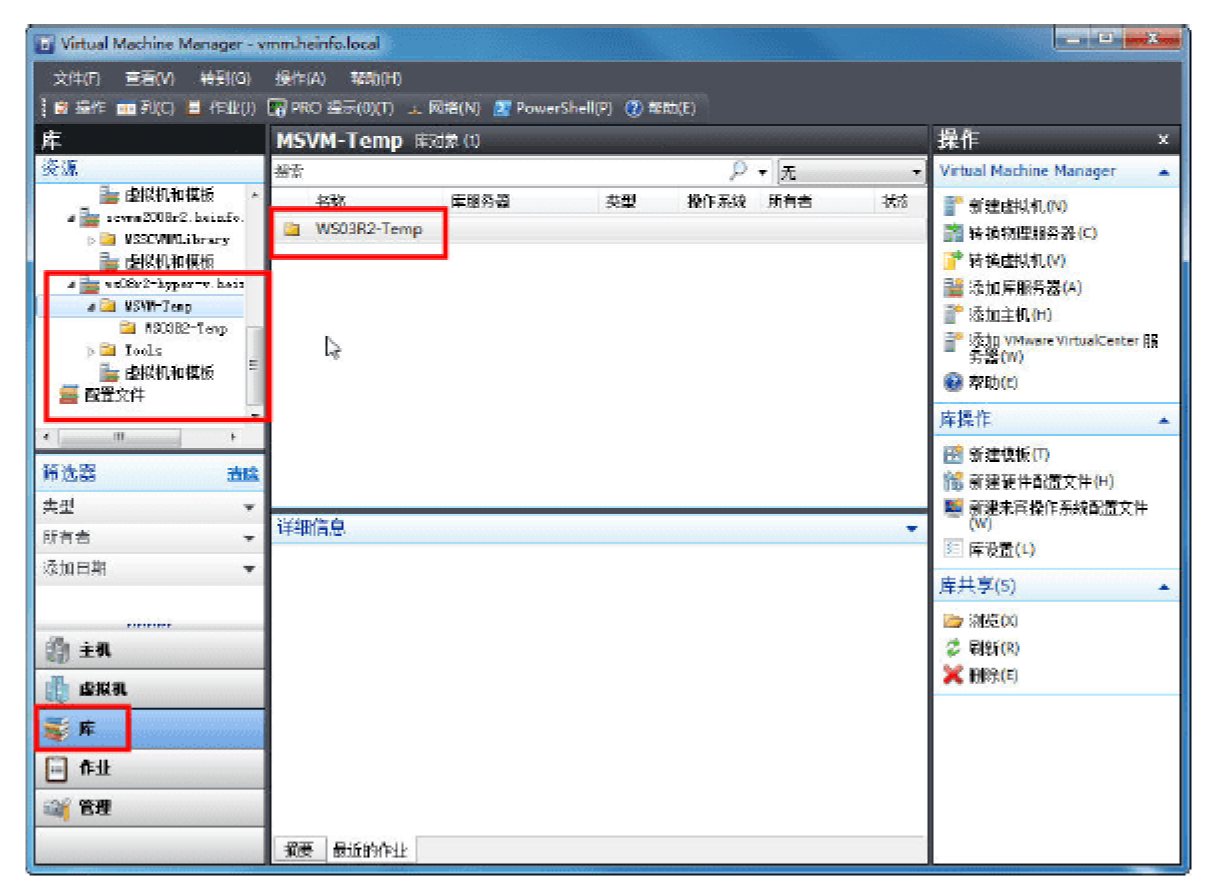


图 12-126　库共享文件夹

12.4.5　从模板部署虚拟机

接下来，介绍怎样使用创建好的模板部署虚拟机，步骤如下。

01 在 VMM 管理员控制台中，在“库→资源”列表中，定位到保存模板的服务器中的“虚拟机和模板”列表，右击选中的模板，在弹出的快捷菜单中选择“新建虚拟机”命令，如图 12-127 所示。

02 在“虚拟机标识”对话框中，设置要部署的新的虚拟机名。，在本例中，设置为 ws03-01，如图 12-128 所示。

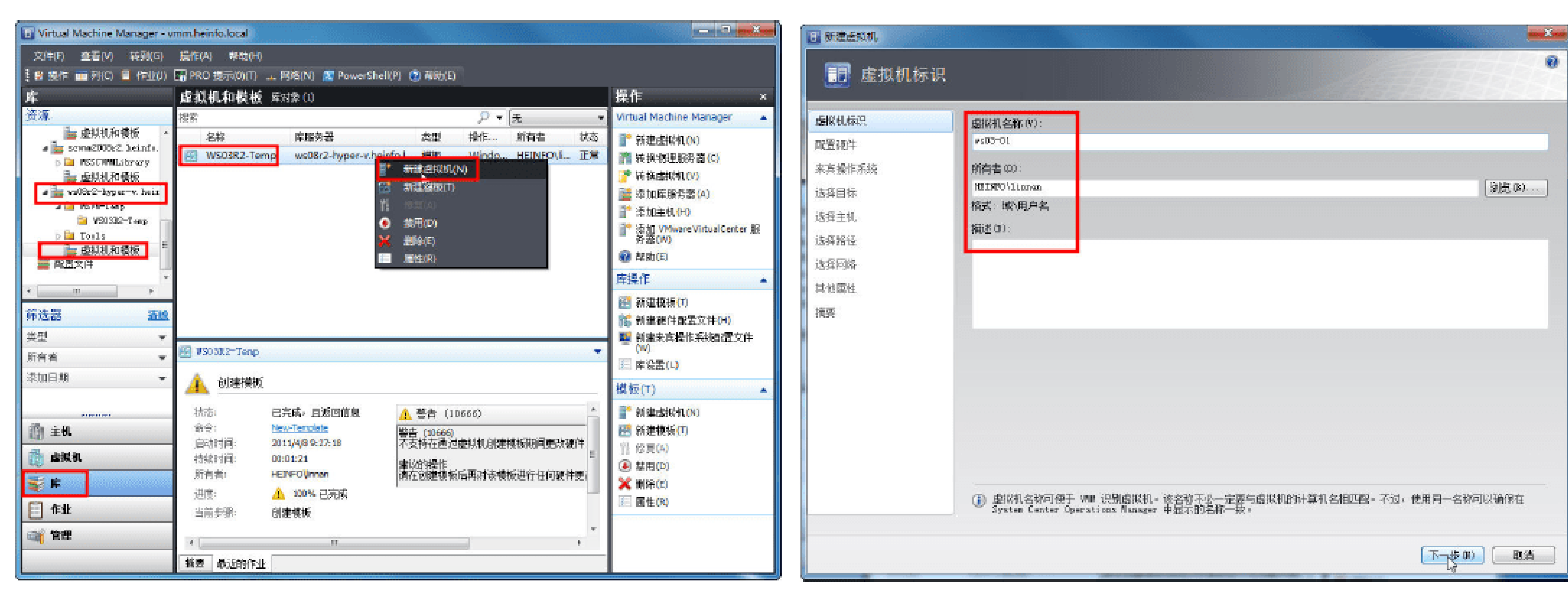


图 12-127　新建虚拟机　　　　图 12-128　虚拟机标识

03 在“配置硬件”对话框中，单击“下一步”按钮，如图 12-129 所示。

04 在“来宾操作系统”对话框中，设置“管理员密码”、“产品密钥”，如图 12-130 所示。

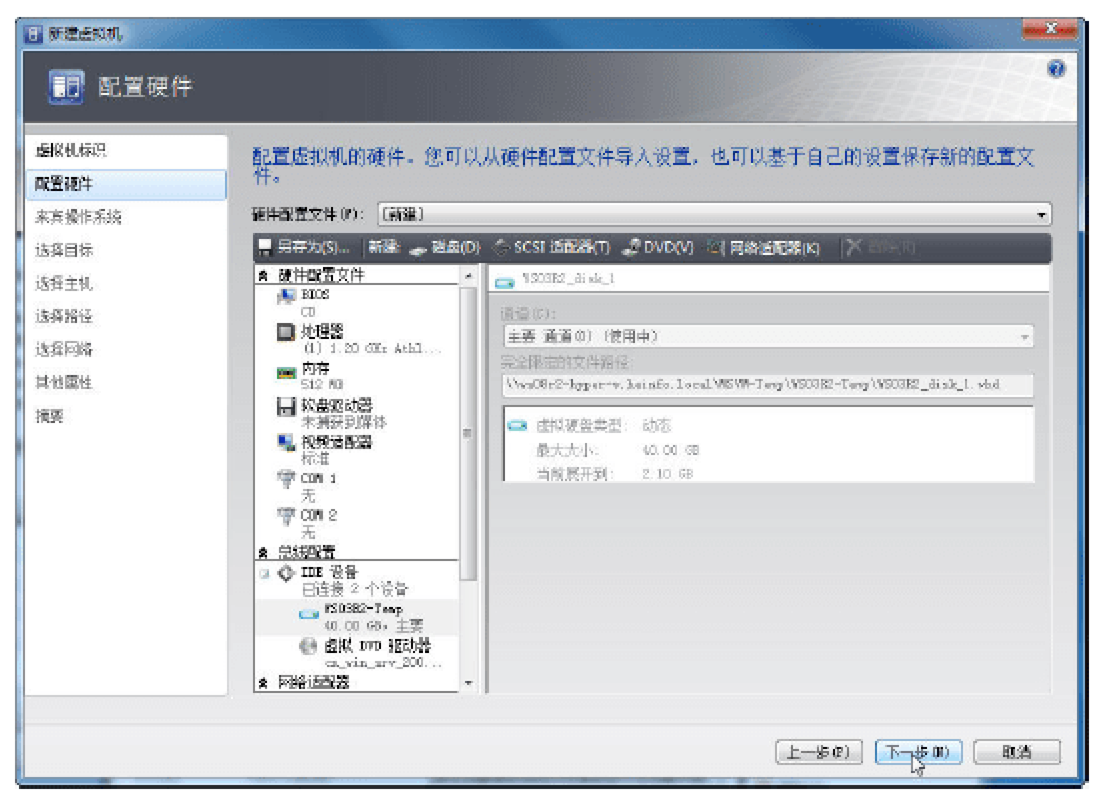


图 12-129　配置硬件

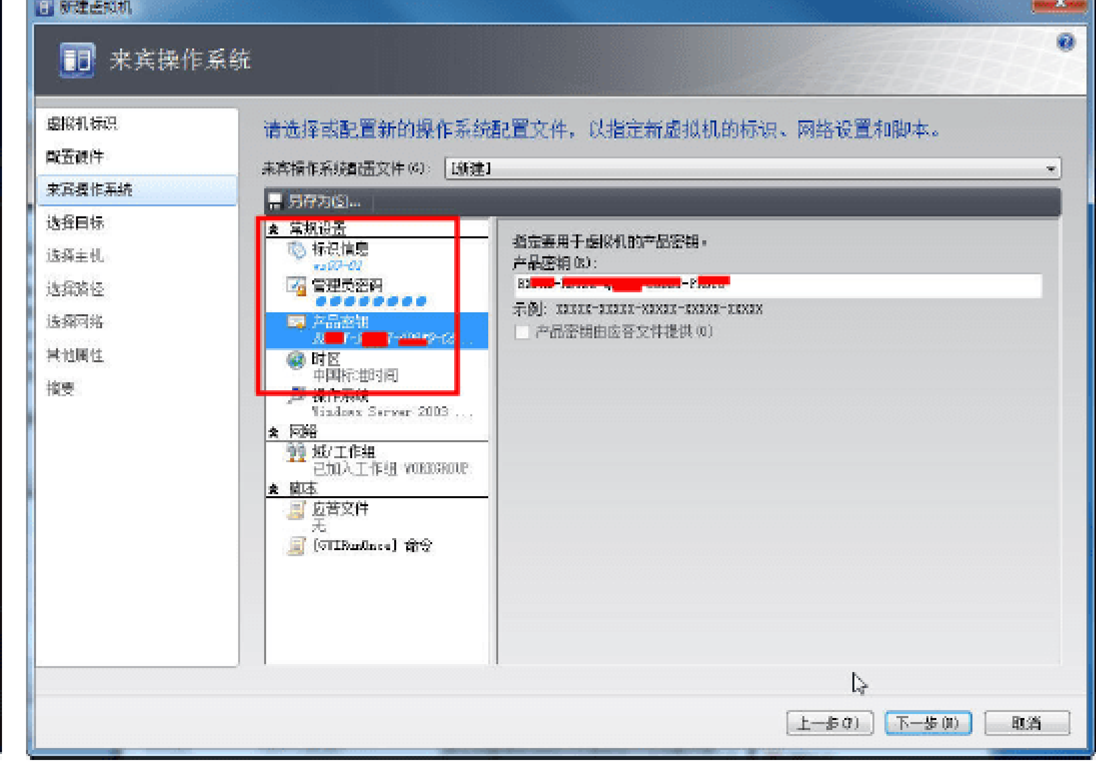
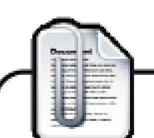


图 12-130　设置管理员密码与产品密钥



说 明

如果不设置管理员密码（自己设置，与源虚拟机的密码无关）与产品密钥，则会弹出图 12-131 的错误信息，并且不能继续。

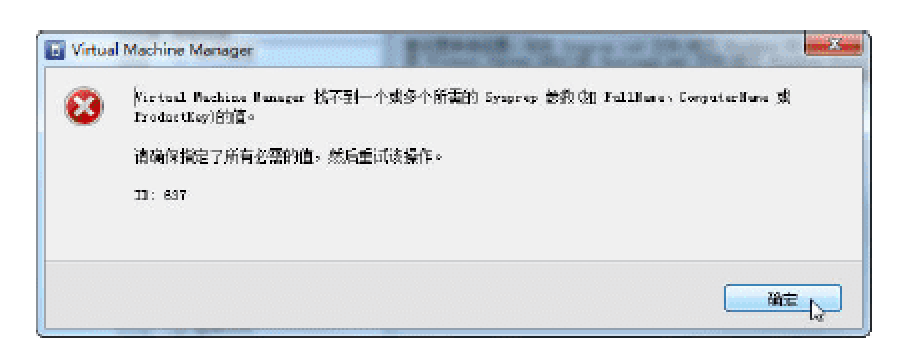


图 12-131　错误信息

05 在设置好管理员密码、产品密钥之后，进入“选择目标”对话框中，选中“将虚拟机放置到主机上”单选按钮，如图 12-132 所示。

06 在“为虚拟机选择主机”对话框中，选择放置虚拟机的物理主机，如图 12-133 所示。可根据需要选择。

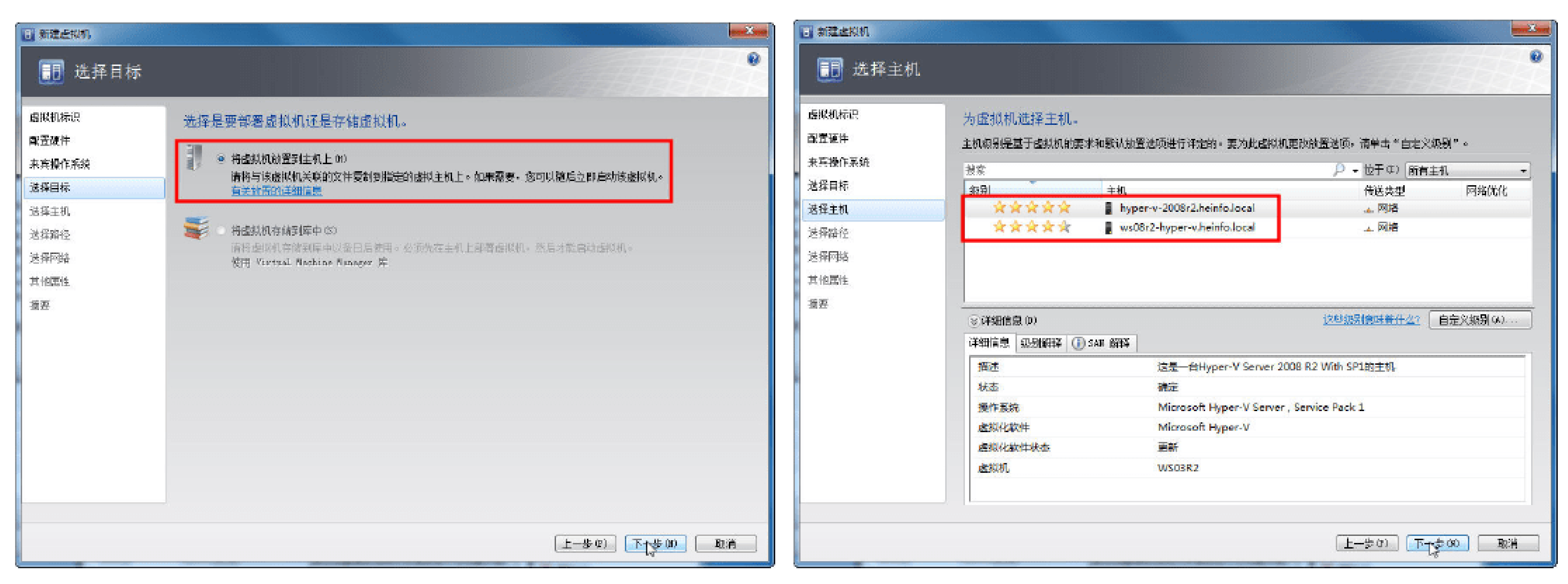


图 12-132　选择目标　　　　图 12-133　为虚拟机选择主机

07 在“选择路径”对话框中，选择虚拟机文件在主机上的存储位置，如图 12-134 所示。

08 在“选择网络”对话框中，指定用于虚拟机的虚拟网络，如图 12-135 所示。

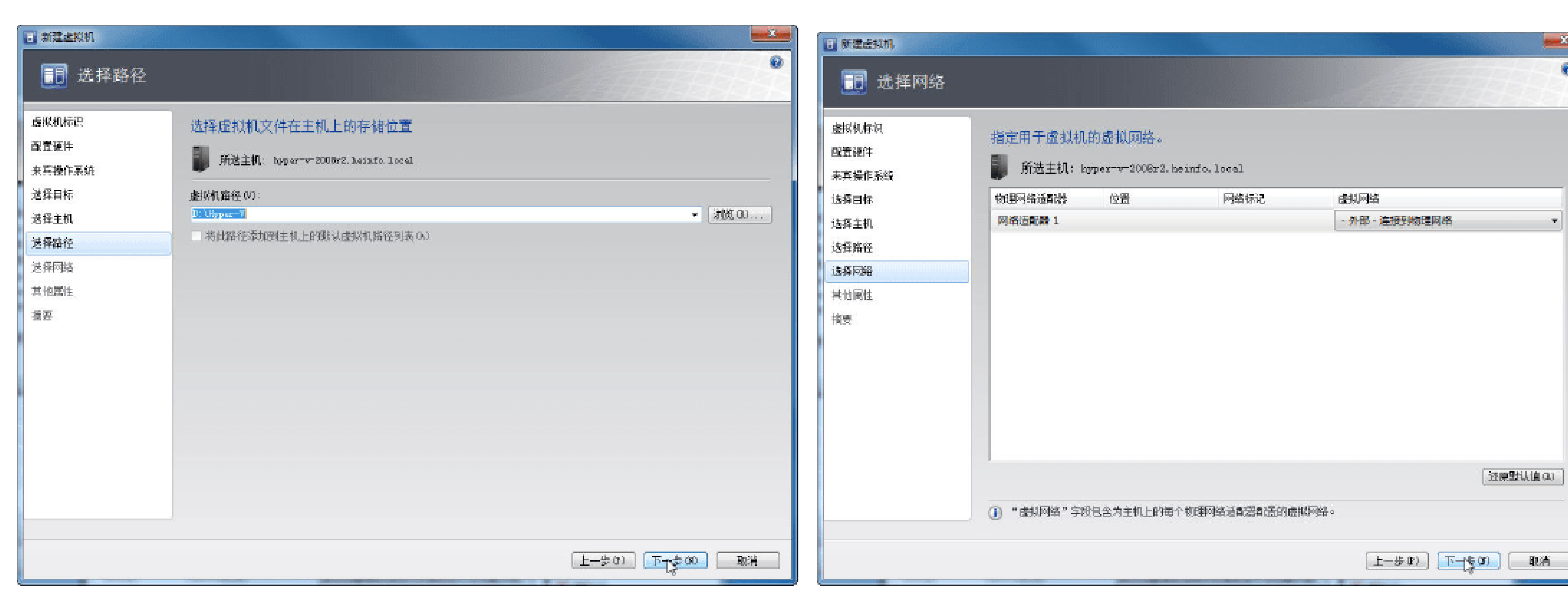


图 12-134　选择路径　　　　图 12-135　选择网络

09 在“其他属性”对话框中，保持默认值，如图 12-136 所示。

10 在“摘要”对话框中，显示从模板部署的新虚拟机的相关信息，如图 12-137 所示。检查无误之后，选中“在主机上部署虚拟机之后启动虚拟机”复选框，然后单击“创建”按钮。

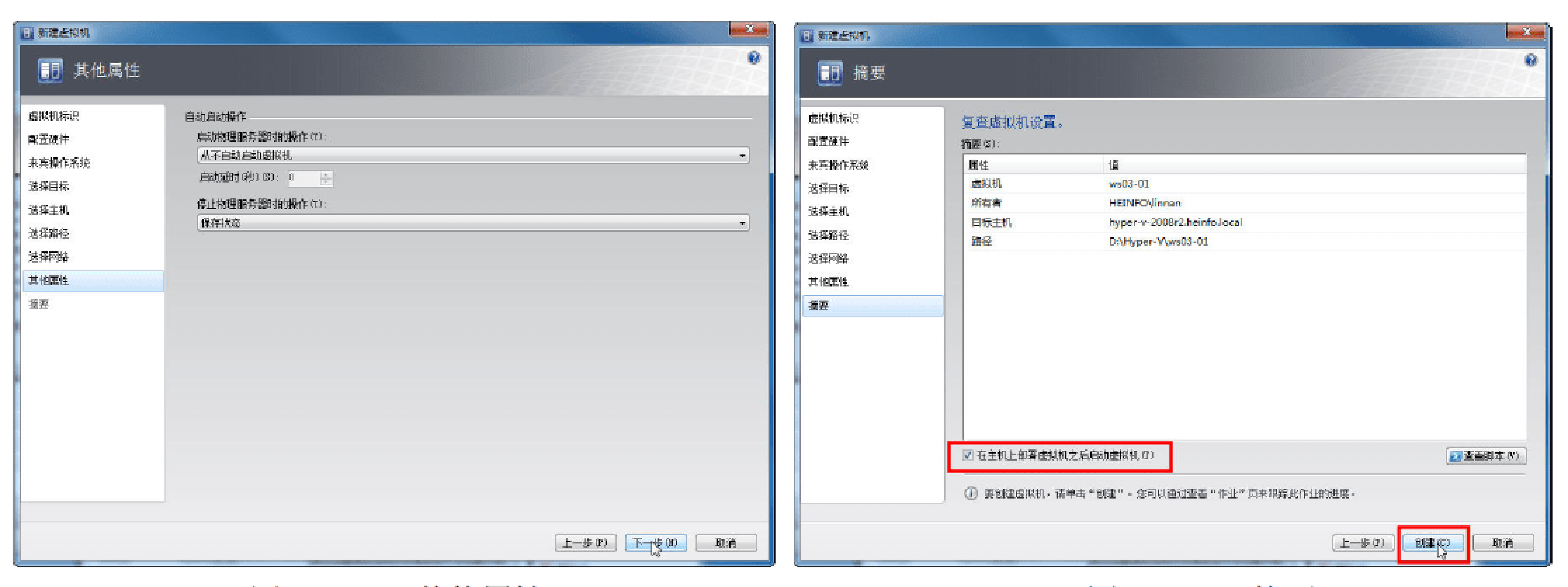


图 12-136　其他属性　　　　图 12-137　摘要

在创建虚拟机的时候，如果在 81%进度的时候出错（如图 12-138 所示），则关闭“作业”窗口，进行下面的操作。

01 在 VMM 管理员控制台，用鼠标右击新创建的虚拟机，在弹出的快捷菜单中选择“连接到虚拟机”命令，如图 12-139 所示。

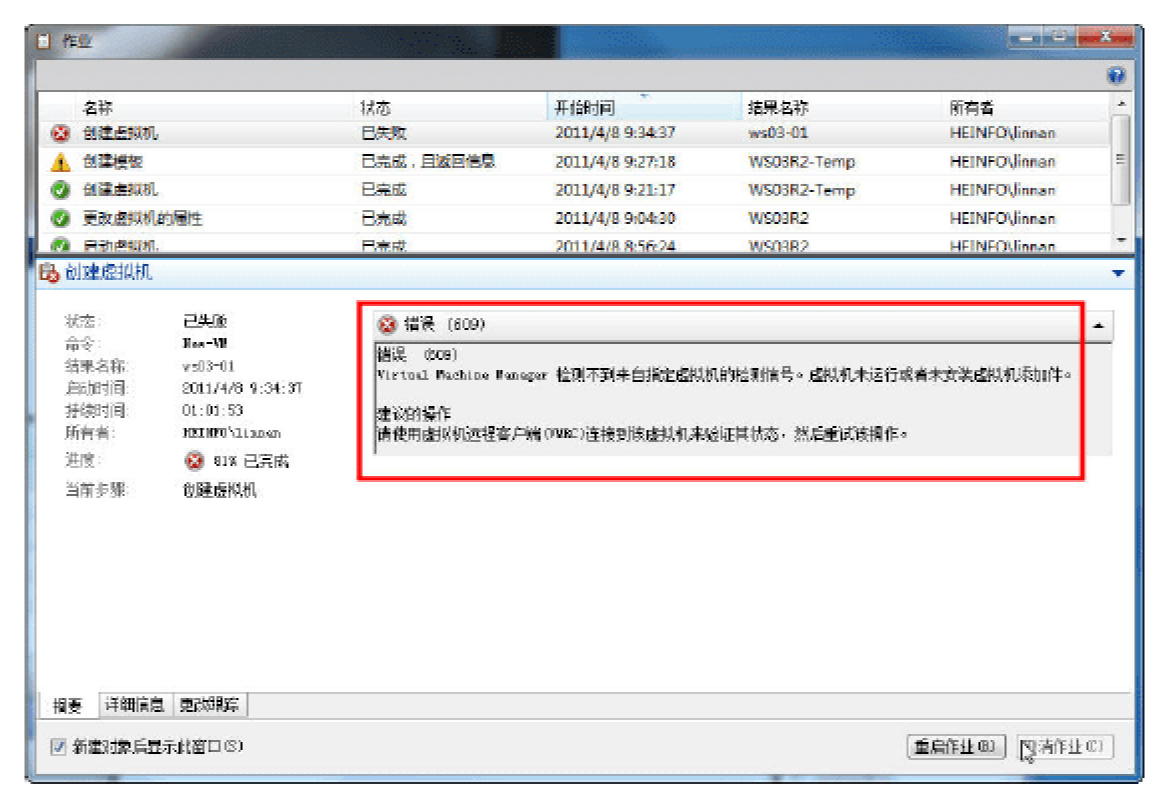


图 12-138 作业



图 12-139 连接到虚拟机

02 进入虚拟机之后，输入管理员密码登录，如图 12-140 所示。管理员密码是图 12-130 中设置的密码。

03 然后返回到 VMM 管理员控制台，右击新部署的虚拟机，在弹出的快捷菜单中选择“修复”命令，如图 12-141 所示。

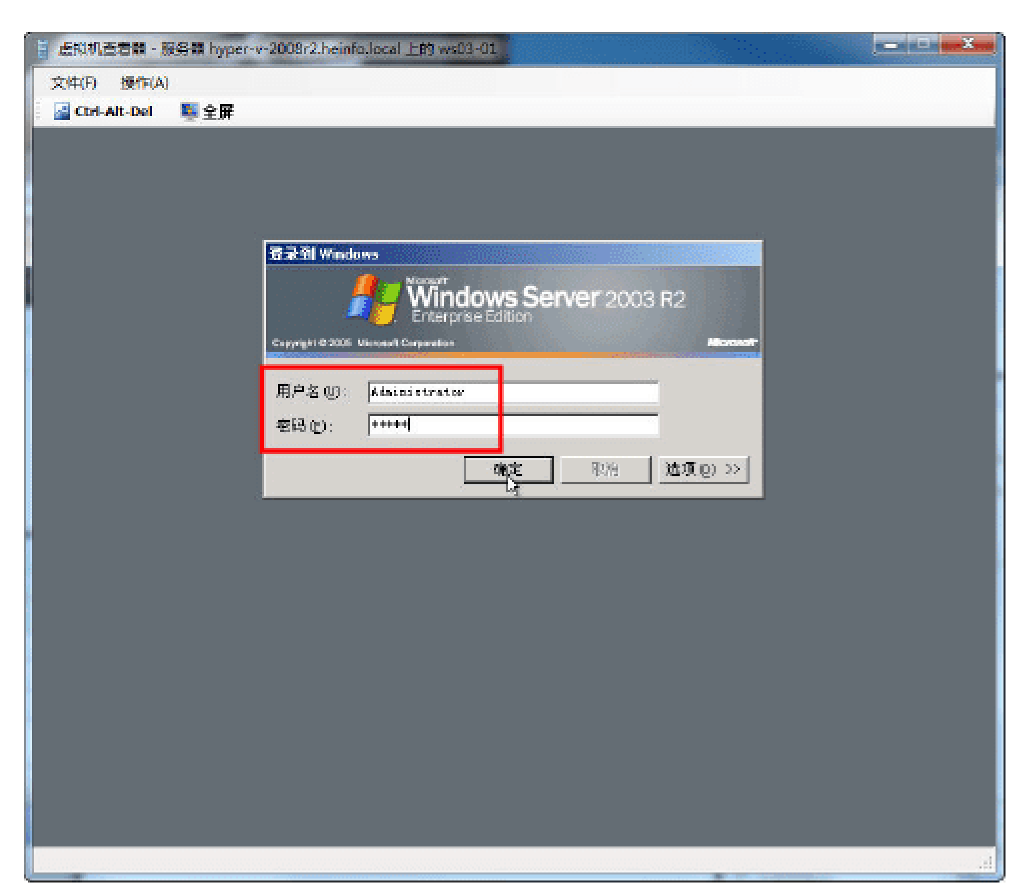


图 12-140 输入管理员密码登录

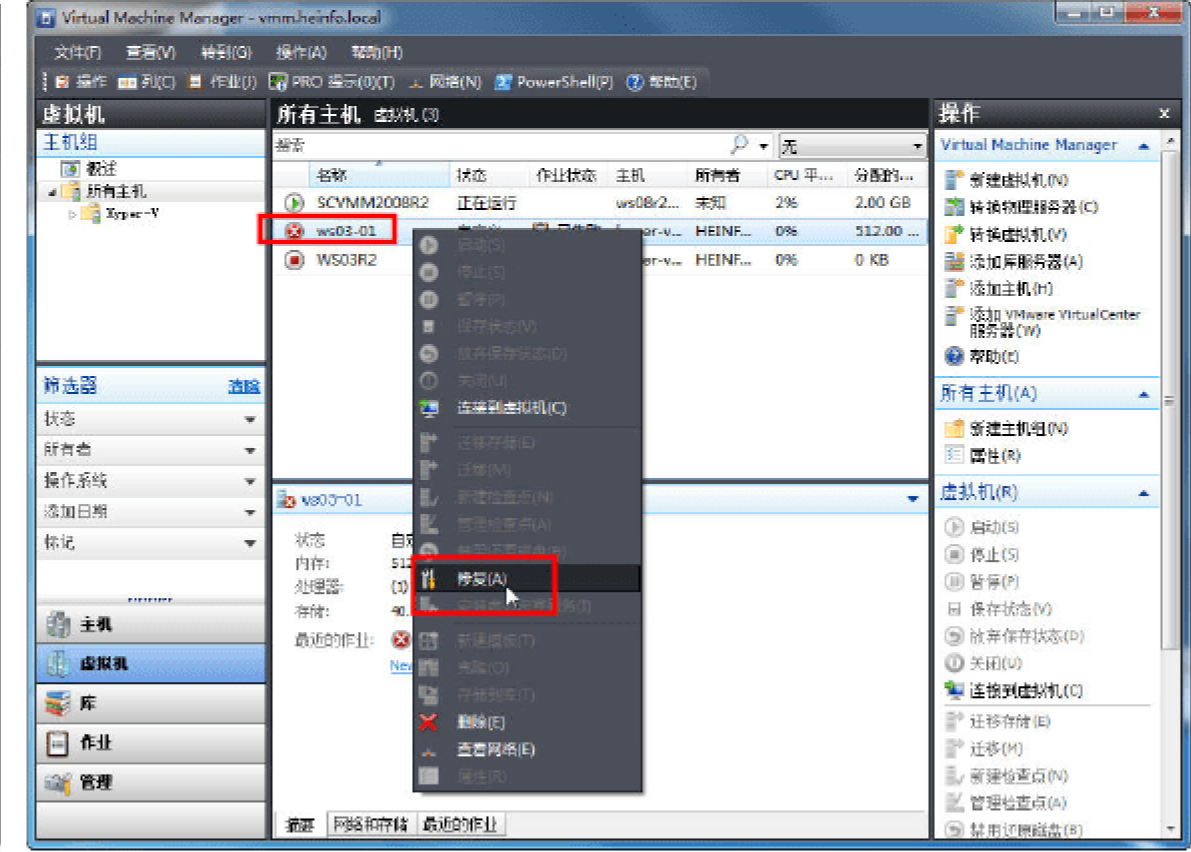


图 12-141 修复

04 在弹出的对话框中，选中“忽略”单选按钮，如图 12-142 所示。

05 最后进入虚拟机查看器，关闭虚拟机，如图 12-143 所示。至此，使用模板部署虚拟机的步骤完成。

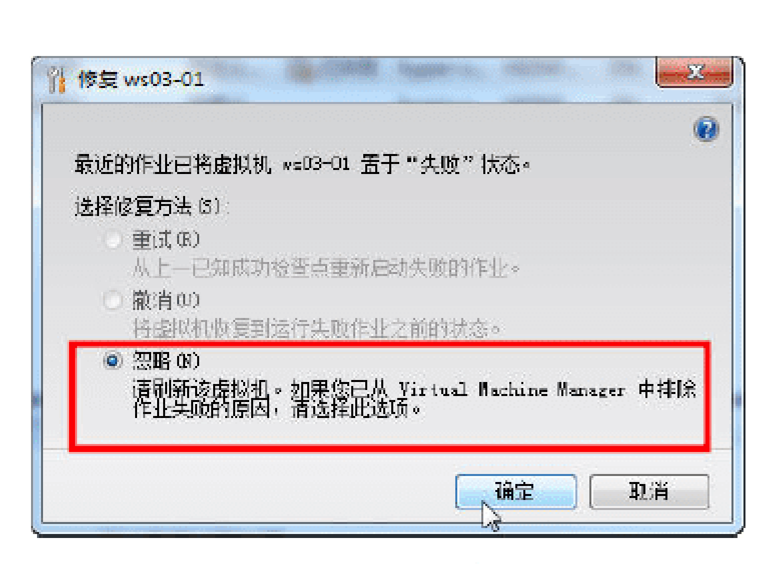


图 12-142 忽略

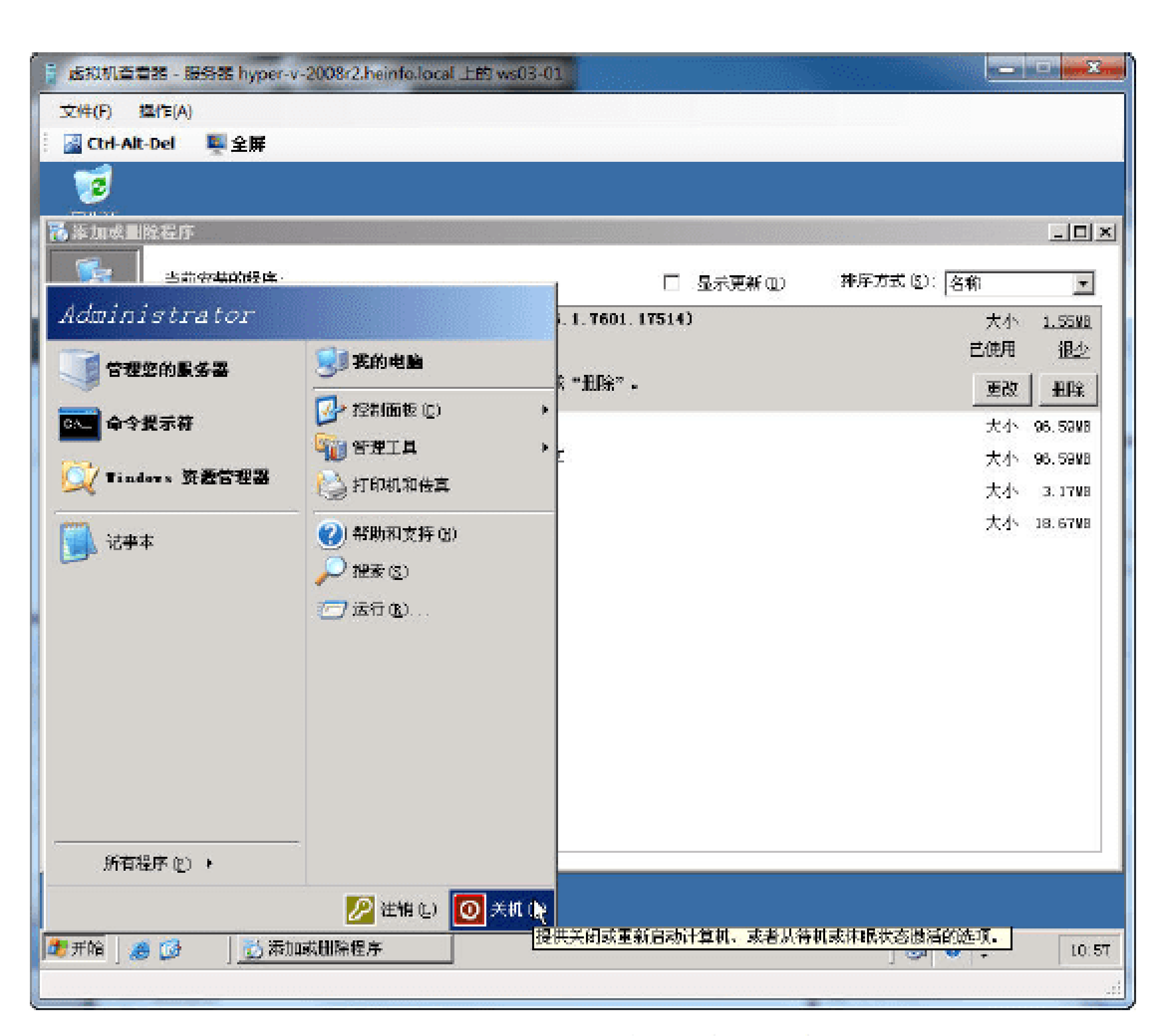


图 12-143 虚拟机关机

12.5 虚拟机的迁移

虚拟机的迁移包括以下几种：

迁移到其他主机：在部署或创建虚拟机的时候，每个虚拟机会“依附”于一个主机，但随着虚拟机的增多，有时候，有的主机负载超过其主机性能，或者是需要对虚拟机进行统一规划或调整的时候，可能需要将虚拟机在不同主机之间迁移。

同一主机迁移到其他存储：当在同一主机上有多个存储时，有的存储空间可能会不能满足虚拟机的运行情况，或者存储空间所属的物理磁盘或存储服务器性能受限，在这种情况下，可以将虚拟机迁移到同一物理主机的其他存储上。

在本次实验中，我们将在网络中部署一台 Windows Storage Server 2008 R2，并从这台存储服务器给 2 台 Hyper-V Server 主机分配空间，然后将原来保存在本地存储中的虚拟机迁移到网络存储，最后在 2 台不同的主机之间迁移虚拟机。

12.5.1 配置 Windows Storage Server 2008 R2

Windows Storage Server 2008 R2 没有单独的产品安装包，它是在 Windows Server 2008 R2 标准版或企业版的基础上，通过安装 Windows Storage Server 2008 R2（以下简称 WSS2008 R2）的软件包实现的。

WSS2008 R2，包括 Windows Storage Server 2008 R2 Workgroup、Windows Storage Server 2008 R2 Standard、Windows Storage Server 2008 R2 Enterprise 3 个版本，其中前 2 个版本需要安装在 Windows Server 2008 R2 标准版上，而 Windows Storage Server 2008 R2 Enterprise 则需要安装在 Windows Server 2008 R2 企业版上，不能将这 3 个产品安装在 Windows Server 2008 R2 的 Web 版与 Datacenter 版本上。

Windows Storage Server 2008 R2 的所有 3 个版本中都支持以下功能：

- iSCSI Software Target 3.3;
- 打印和文档服务;
- Windows 备份;
- Windows 搜索;
- DHCP 服务器;
- 网络文件系统（NFS）;
- 分布式文件系统复制（DFSR）;
- 文件服务器资源管理器（FRSM）。

WSS2008 R2 的功能及指标如表 12-1 所示：

表 12-1　WSS2008 R2 的功能及指标

说明	Workgroup Edition	Standard Edition	Enterprise Edition
随机存取内存(RAM)	32GB	32GB	2TB
网络适配器	2	无限制	无限制
磁盘(数量/接口/RAID 类型)	6/任意/任意	任意/任意/任意	任意/任意/任意
用户	25	无限制	无限制
服务器消息块(SMB)连接	50	无限制	无限制
单实例存储(SIS)	否	是	是
故障转移群集	否	是	是
DNS 和 WINS	否	是	是
RODC	否	是	是
虚拟化(Hyper-V)	否	是	是
托管缓存	否	否	是

下面简要介绍 Windows Storage Server 2008 R2 的安装，以及为两台 Hyper-V Server 分配存储空间的步骤。

1. 安装 WSS 2008 R2

WSS2008 R2 的安装比较简单，我们以安装 Windows Storage Server 2008 R2 Enterprise 为例进行介绍，主要过程如下。

01 安装 Windows Server 2008 R2 企业版，并激活（当然也可以在安装 WSS2008 R2 组件之后激活），如图 12-144 所示。



图 12-144　安装 WS2008 R2 企业版

02 加载 WSS2008 R2 软件包镜像，并运行“Windows Storage Server 2008 R2”目录中的“Windows6.1-KB982050-x64-EnterpriseBranding.MSU”组件（这是 WSS2008 企业版组件），如图 12-145、图 12-146 所示。其他几个组件可以根据需要选择。

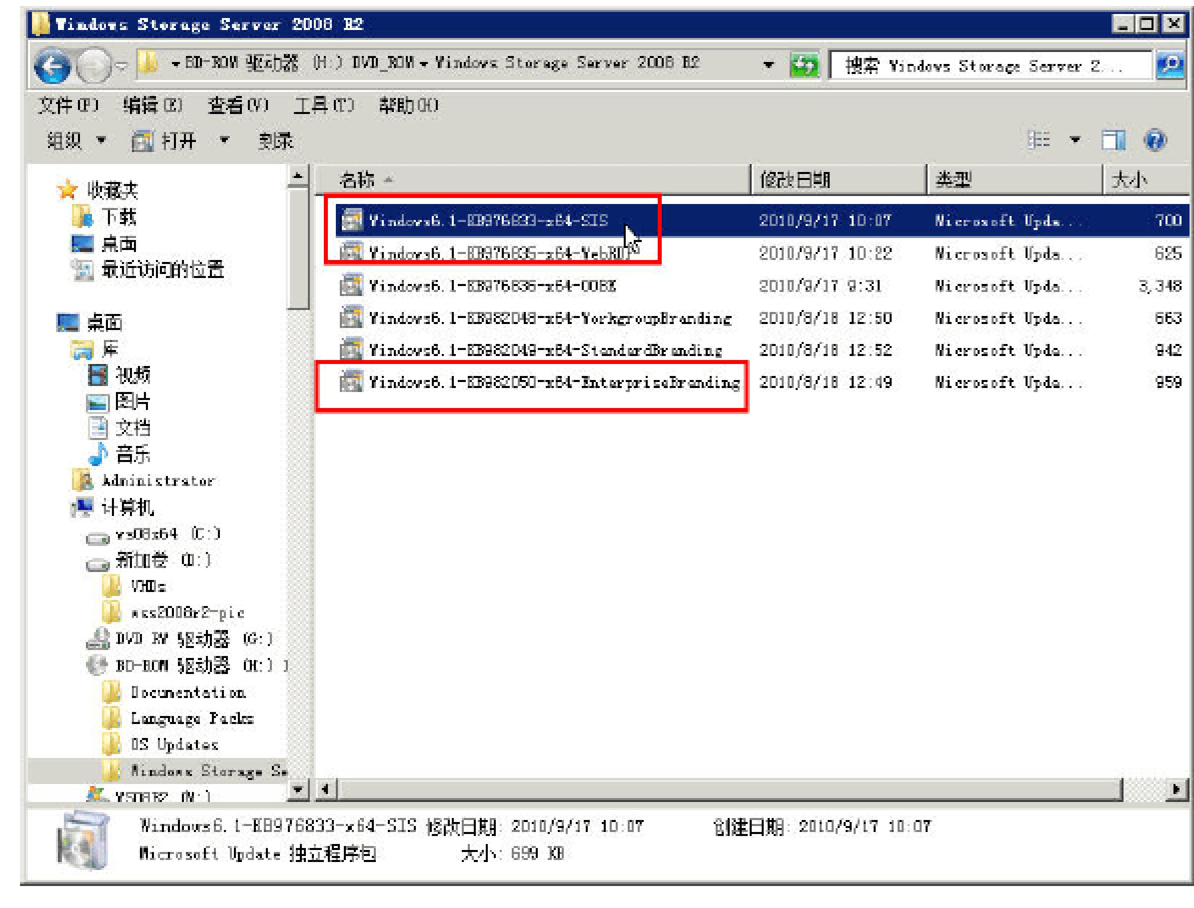


图 12-145　WSS2008 R2 安装文件

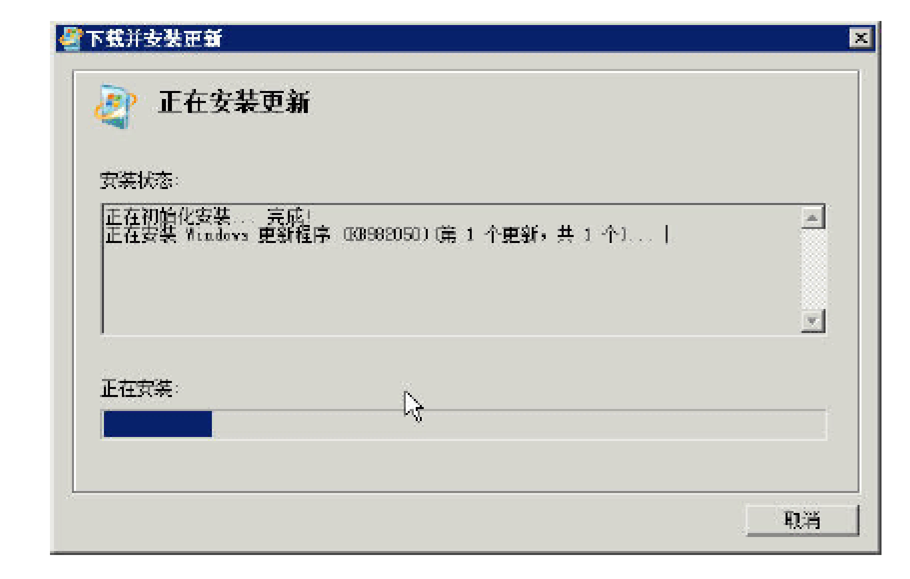


图 12-146　安装 WSS2008 R2 核心部件

安装完成之后，根据提示重新启动计算机，再次进入系统之后，在“帮助”菜单可以看到，当前系统已经是 Windows Storage Server 2008 R2，如图 12-147 所示。

03 加载 iSCSI_Software_Target_33.iso 镜像，运行其中的“iscsitarget.msi”程序（如图 12-148 所示），这是“Microsoft iSCSI Software Target”程序。



图 12-147　升级完成

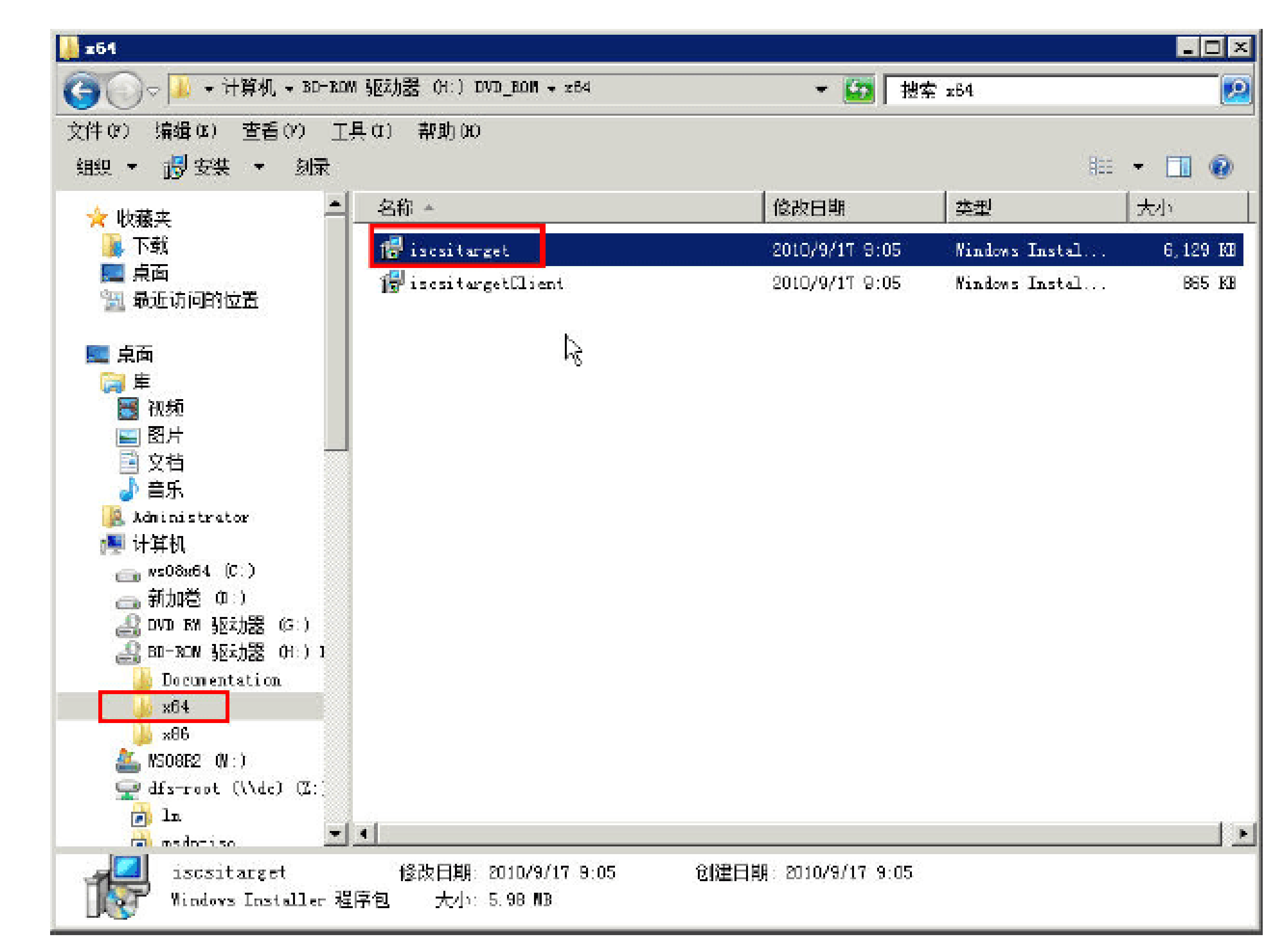


图 12-148　iscsitarget.msi 程序

04 安装过程很简单，按照默认值即可完成安装，如图 12-149 所示。

在 WSS2008 R2 的安装光盘中，还有一些补丁与程序，可以根据需要安装。

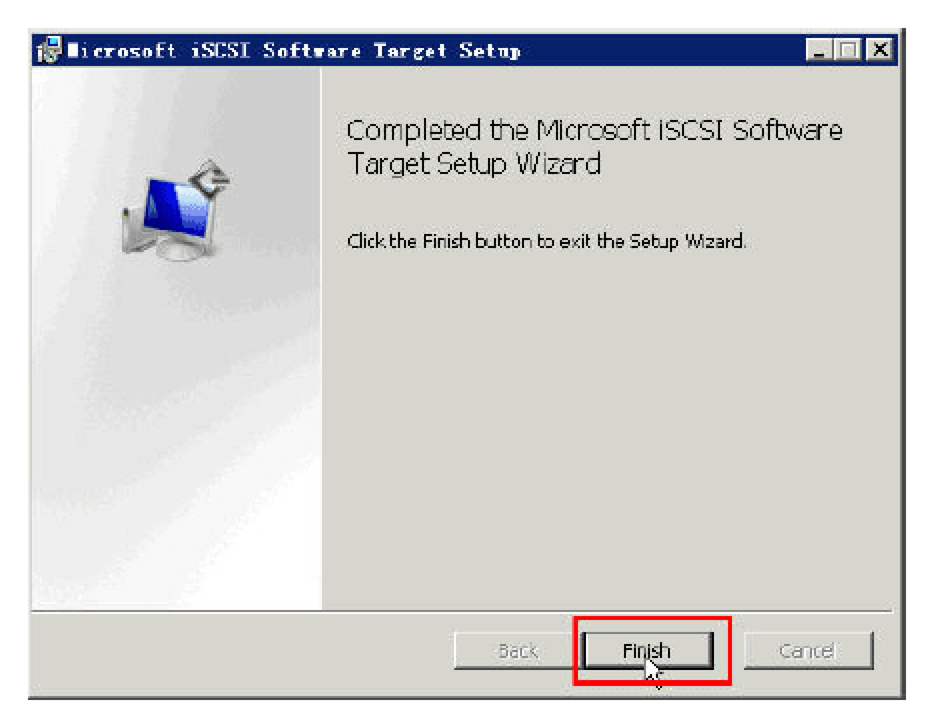


图 12-149　安装完成

2. 为 Hyper-V 分配存储空间

安装好 iscsitarget.msi 之后，就可以为 Hyper-V（或网络中的其他 Windows、Linux 操作系统服务器）分配网络空间了，下面以为 172.30.5.17、172.30.5.31 分配空间为例，介绍配置方法。

01 在 WSS2008 R2 服务器中（本例中，该服务器 IP 地址为 172.30.5.5），运行“Microsoft iSCSI Software Target”，如图 12-150 所示。

02 在“iSCSITarget”控制台中右击“iSCSI 目标”，在弹出的快捷菜单中选择“创建 iSCSI 目标”命令，如图 12-151 所示。



图 12-150　运行“Microsoft iSCSI Software Target”

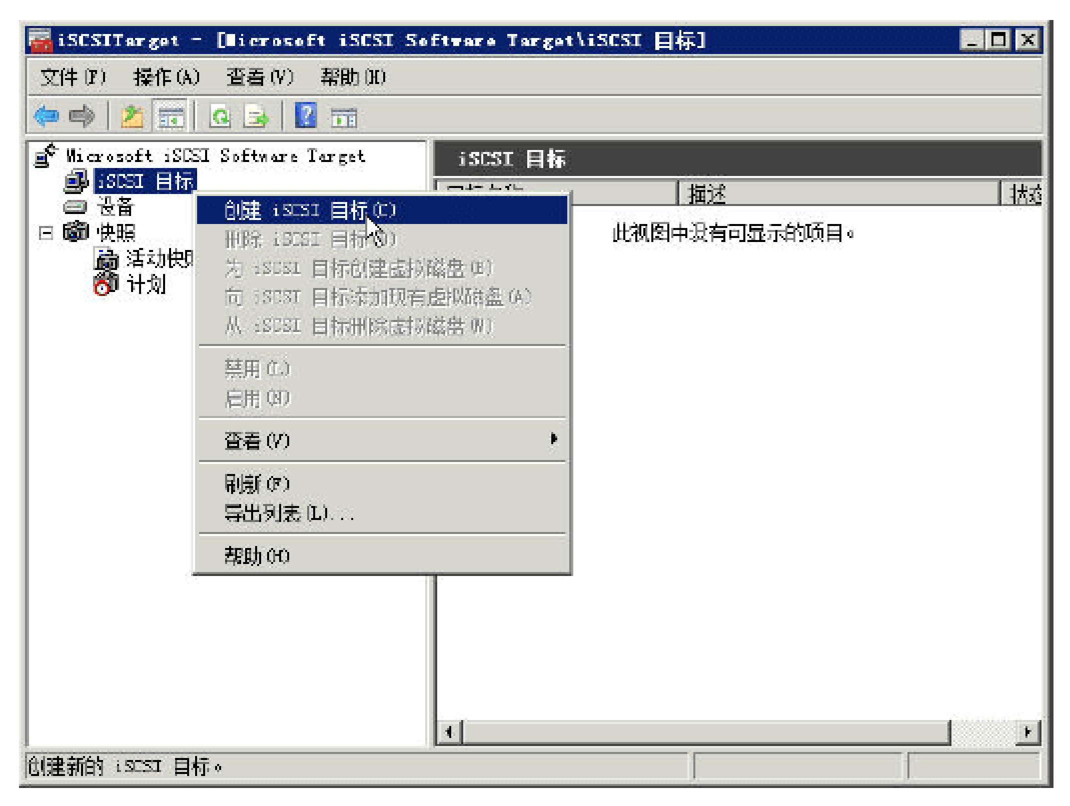


图 12-151　创建 iSCSI 目标

03 在“欢迎使用‘创建 iSCSI 目标向导’”对话框，单击“下一步”按钮，如图 12-152 所示。

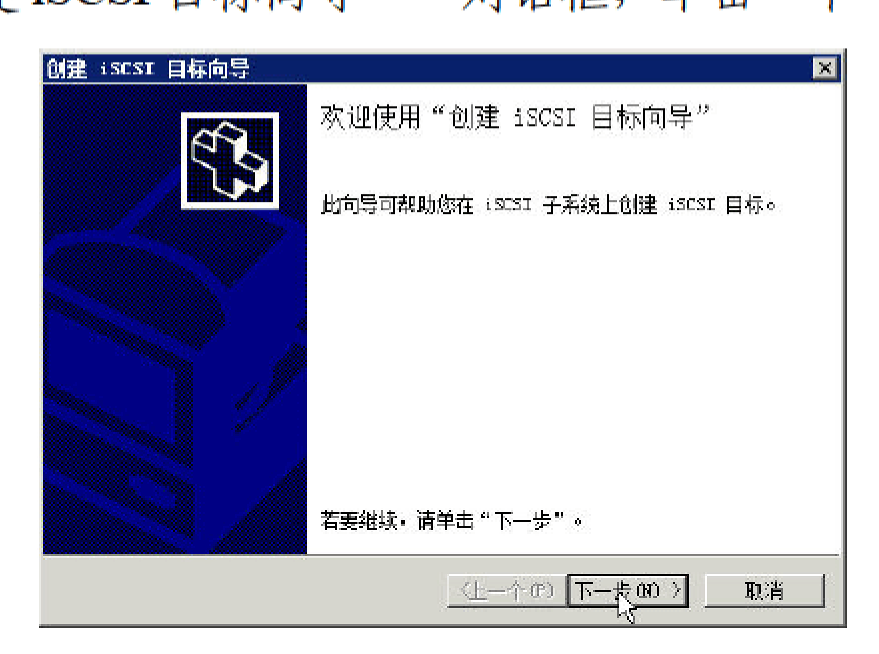


图 12-152　创建 iSCSI 目标向导

04 在“iSCSI 目标标识”对话框中，在“iSCSI 目标名称”文本框中，为新创建的 iSCSI 目标创建一个名称，在本例中为“Hyper-V”，如图 12-153 所示，单击“下一步”按钮。

05 在“iSCSI 发起程序标识符”对话框中，单击“高级”按钮，在弹出的“高级标识符”对话框中，单击“添加”按钮，在“添加/编辑标识符”对话框中，在“标识符类型”下拉列表中选择“IP 地址”，在“值”处输入第 1 台 Hyper-V 主机的 IP 地址 172.30.5.17，然后单击“确定”按钮返回“高级标识符”对话框，再次单击添加按钮，添加 172.30.5.31 的 IP 地址，如图 12-154 所示。



图 12-153　iSCSI 目标标识

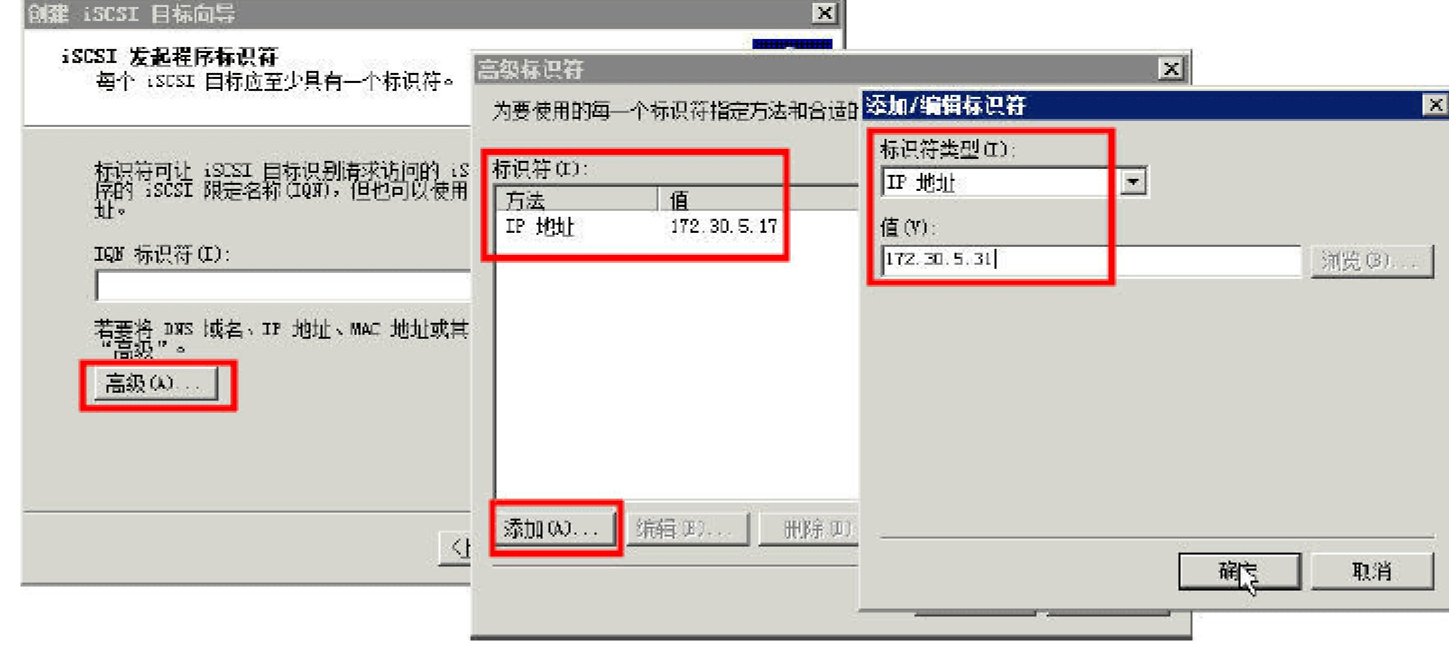


图 12-154　添加 IP 地址标识符

添加之后单击“下一步”按钮，再次单击“完成”按钮，完成添加，如图 12-155 所示。



图 12-155　完成分配

12.5.2　在 Windows Server 2008 R2 中添加 iSCSI 存储

在配置了 Windows Storage Server 2008 R2 并为 2 台 Hyper-V 主机分配了存储空间之后，接下来，需要在 2 台主机中，添加并使用存储。首先介绍在 Windows Server 2008 R2 With Hyper-V 主机中的添加方法与步骤。

01 在 Windows Server 2008 R2 With Hyper-V 的主机中，在“管理工具”中选择“iSCSI 发起程序”命令，如图 12-156 所示。

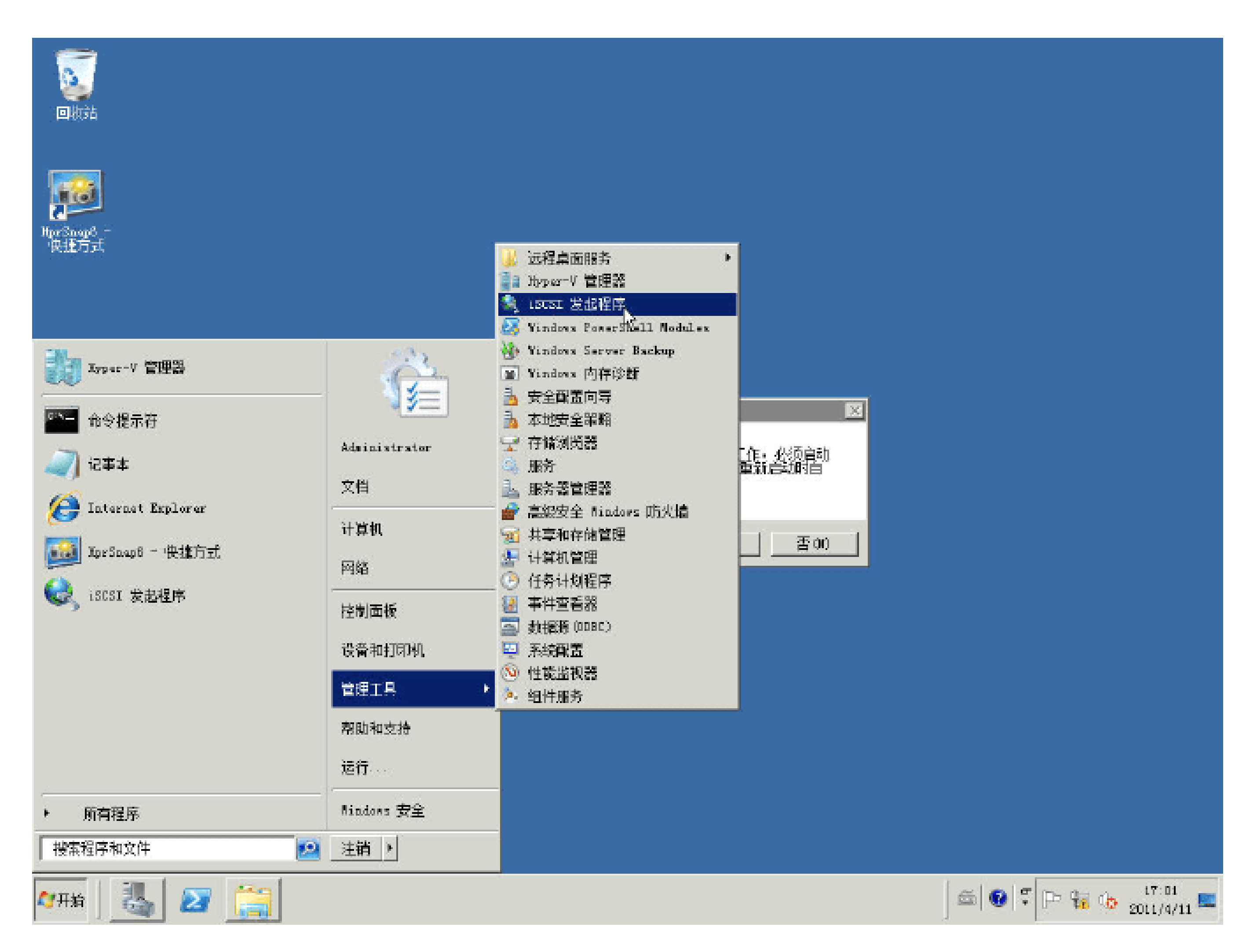


图 12-156　iSCSI 发起程序

02 在“iSCSI 发起程序　属性”对话框中，在“发现”选项卡中，单击“发现门户”按钮，在弹出的“发现目标门户”对话框中，在“IP 地址或 DNS 名称”文本框中，输入 Windows Storage Server 2008 R2 的 IP 地址，本例中是 172.30.5.5，然后单击“确定”按钮，如图 12-157 所示。

03 在“目标”选项卡中，在“已发现的目标”列表中，可以看到添加的 iSCSI 发起目标，但该目标的“状态”是“不活动”，单击“连接”按钮，如图 12-158 所示。

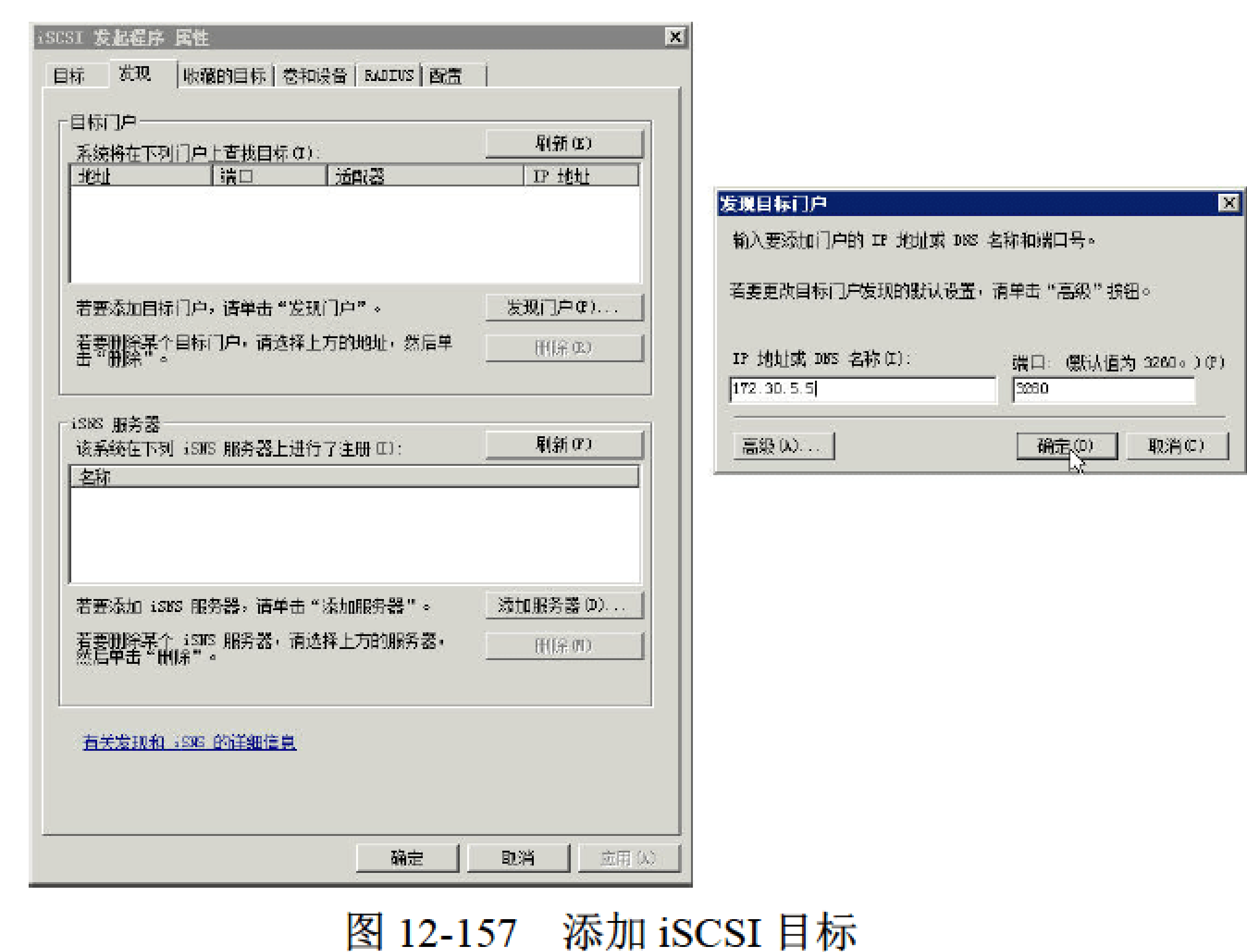




图 12-157　添加 iSCSI 目标

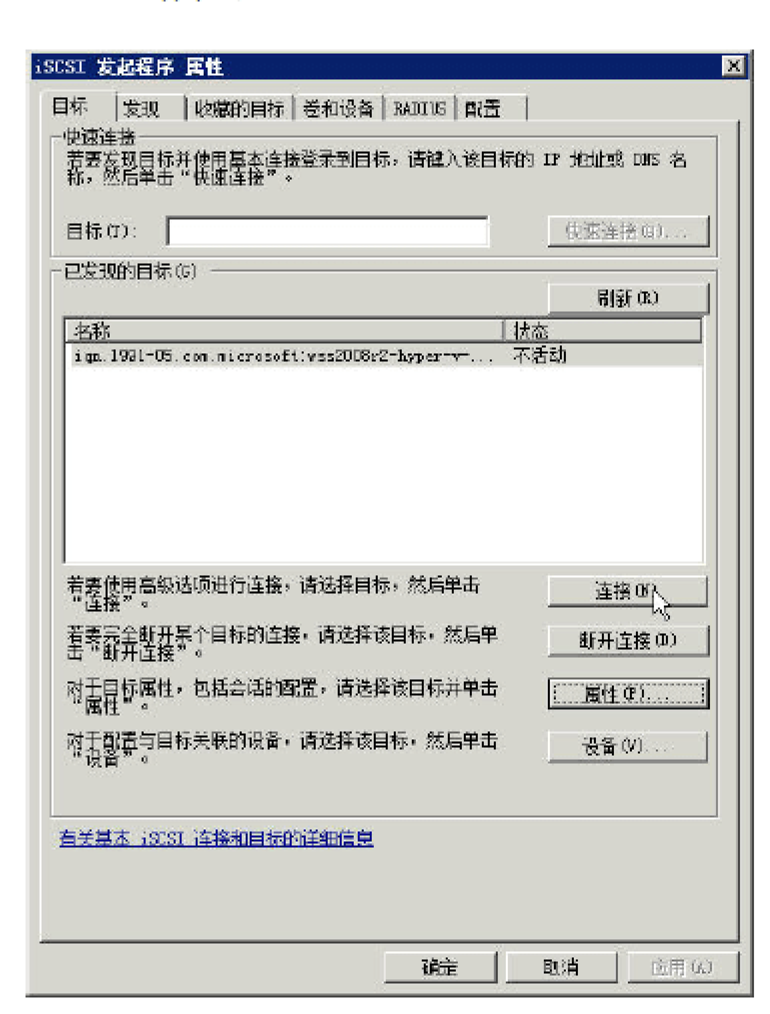


图 12-158　连接

04 在弹出的“连接到目标”对话框中，选中“将此连接添加到收藏目标列表”与“启用多路径”复选框，然后单击“确定”按钮，如图 12-159 所示。

05 再次返回到“iSCSI 发起程序　属性”对话框，发现 iSCSI 目标的状态是“已连接”，如图 12-160 所示。单击“确定”按钮返回。

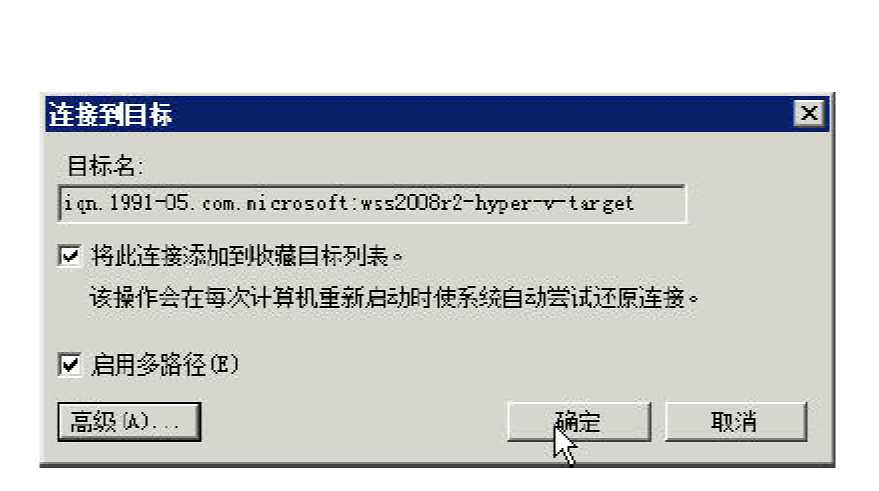


图 12-159 连接到目标

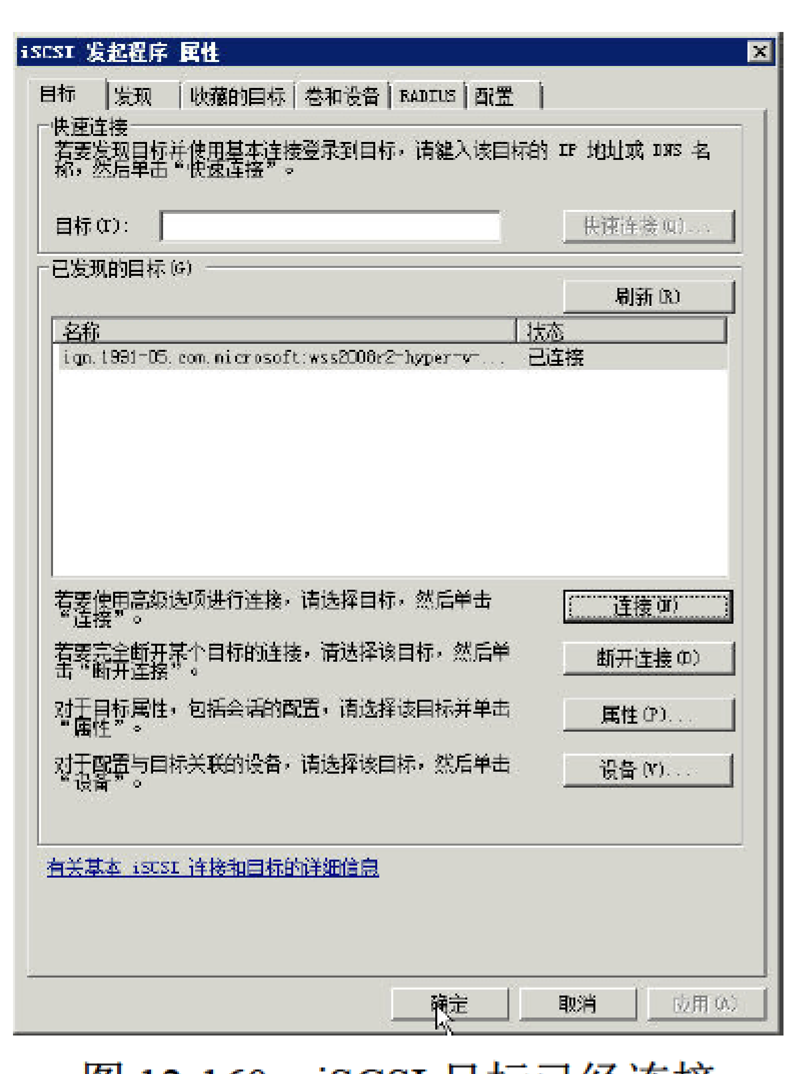


图 12-160 iSCSI 目标已经连接

在添加 iSCSI 目标之后，此时在计算机中已经多添加了一块新的“网络”硬盘，该硬盘对于操作系统来说，相当于“本地硬盘”，需要对此硬盘进行分区、格式化等操作，步骤如下。

01 打开“服务器管理器”窗口，定位到“存储→磁盘管理”，在右侧的列表中，可看到新增加的硬盘，用鼠标右键单击，在弹出的快捷菜单中选择“联机”命令，等硬盘联机后，再用鼠标右键单击，从弹出的快捷菜单中选择“初始化磁盘”命令，如图 12-161 所示。

02 在弹出的“初始化磁盘”对话框中，选中要初始化的磁盘，在“为所选磁盘使用以下磁盘分区形式”中，选择“GPT（GUID 分区表）”单选按钮，如图 12-162 所示。

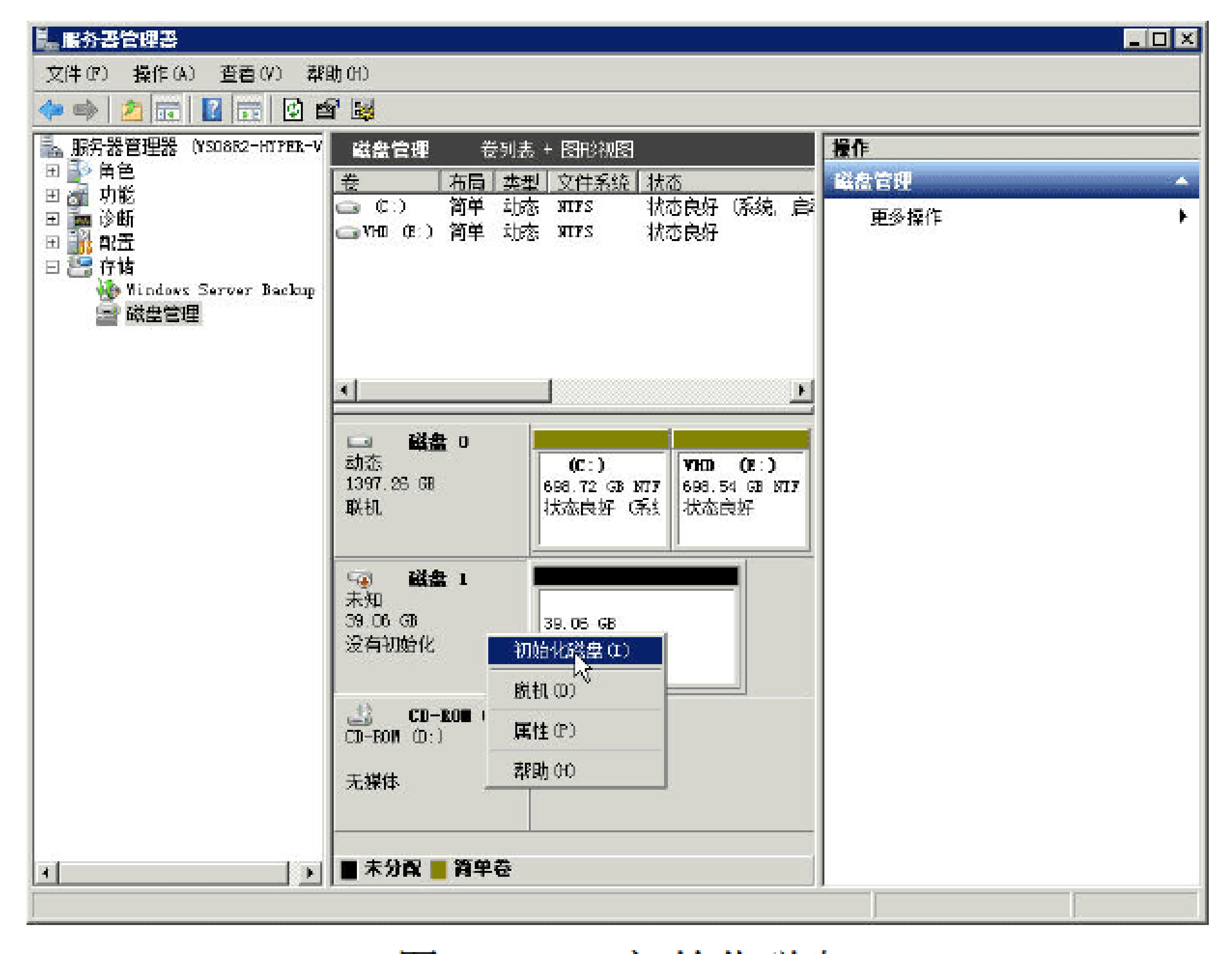


图 12-161 初始化磁盘

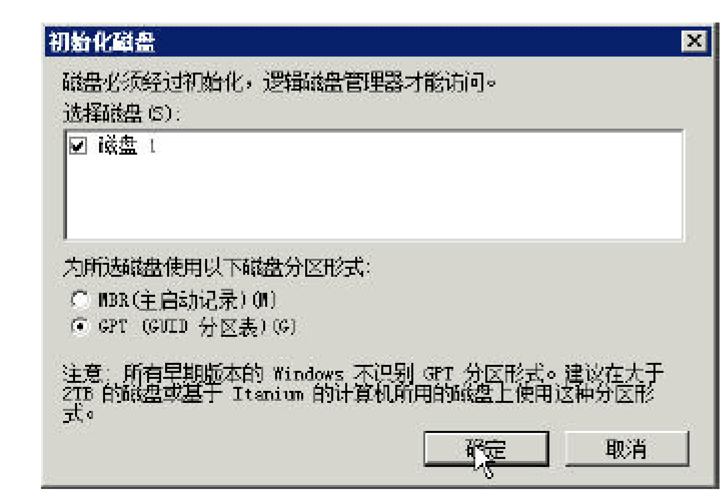


图 12-162 初始化磁盘

03 之后对此硬盘新建简单卷，并分配盘符（本例中为 P，如图 12-163 所示），然后使用 NTFS 文件系统格式化（如图 12-164 所示），格式化之后即可使用。

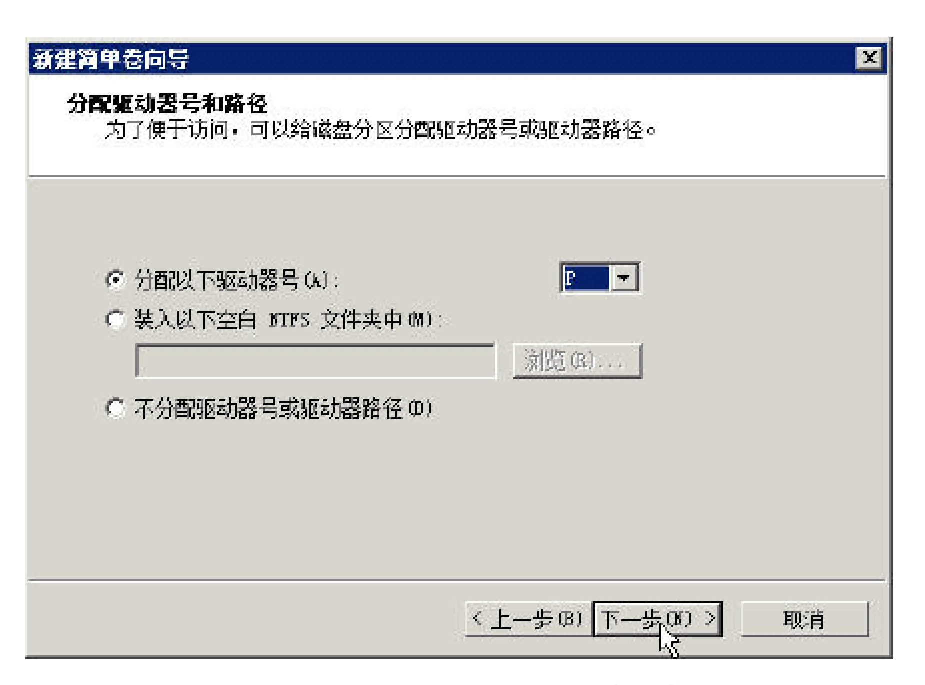


图 12-163　分配盘符

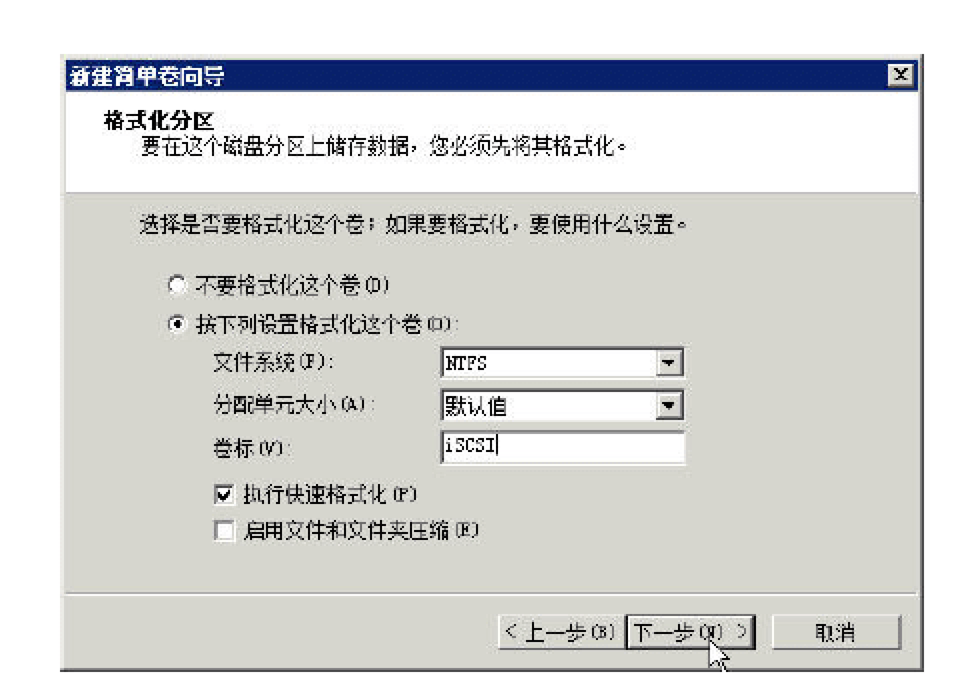


图 12-164　格式化

12.5.3　在 Hyper-V Server 2008 R2 中添加 iSCSI 存储

在 Hyper-V Server 2008 R2 中添加 iSCSI 存储，从本质上来说，与在 Windows Server 2008 R2 中是一致的。但由于 Hyper-V 默认是“文本界面”，所以在添加的时候，会略有区别。下面分别介绍。

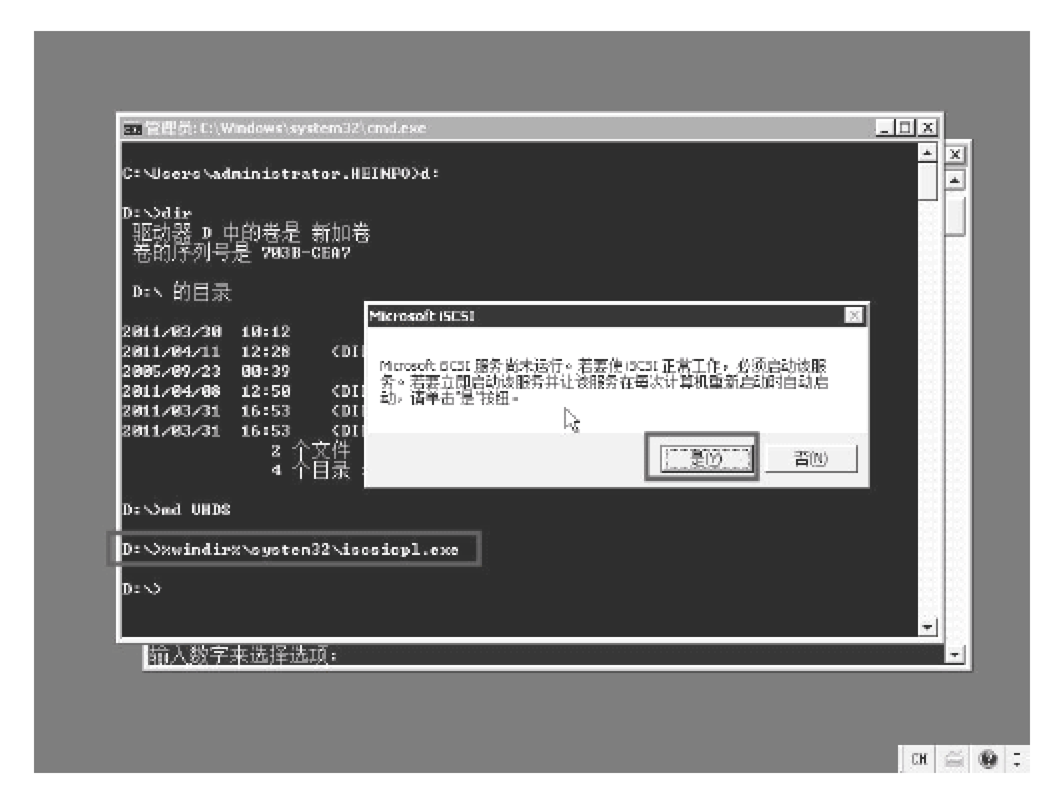


图 12-165　运行 iSCSI 发起程序

01 在 Hyper-V Server 2008 R2 中，在“命令提示符”窗口中，执行“%windir%\system32\iscsicpl.exe”程序，进入“Microsoft iSCSI”程序，在弹出的对话框中，单击“是”按钮，如图 12-165 所示。

02 然后进入“iSCSI 发起程序 属性”对话框，参照 12.5.2 节的内容，添加 iSCSI 服务器端并进行连接，如图 12-166、图 12-167 所示。

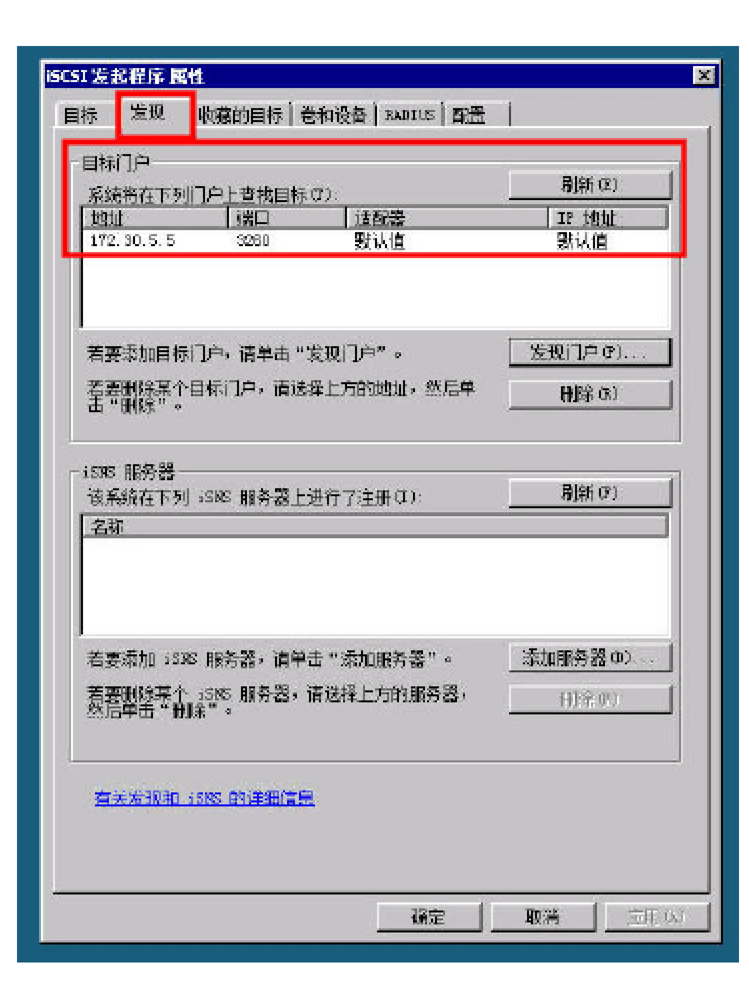


图 12-166　添加 iSCSI 服务器

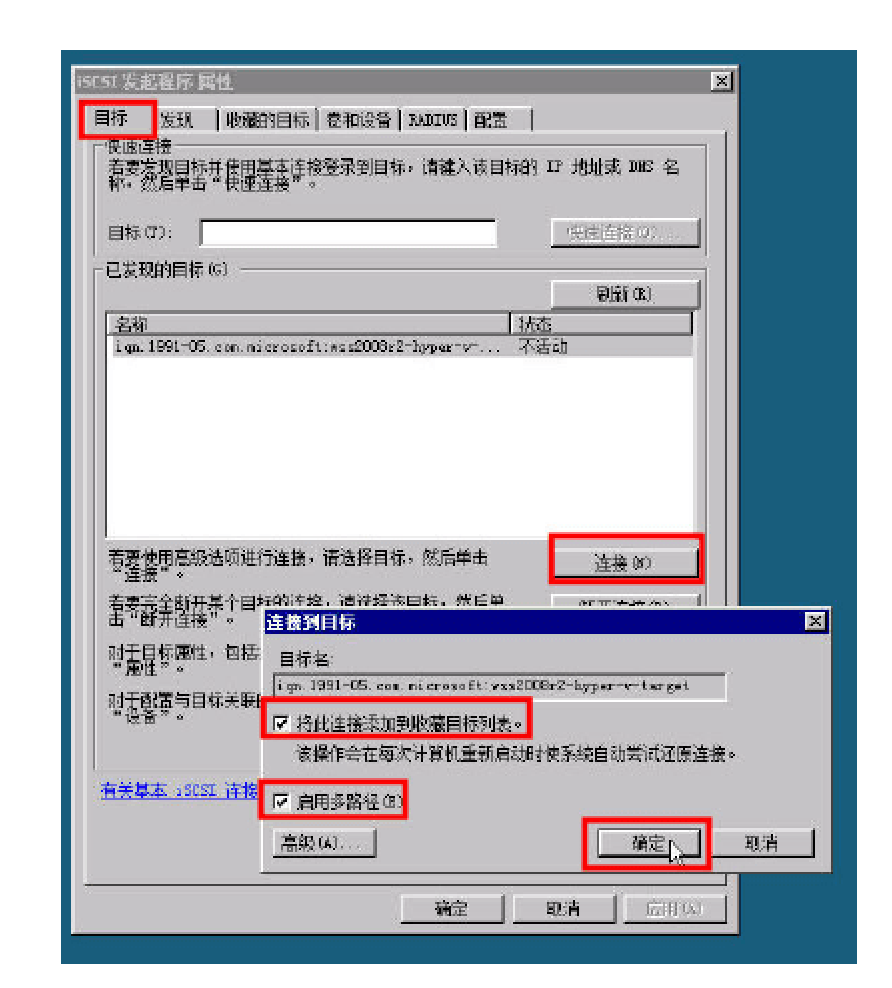


图 12-167　连接到 iSCSI 服务器

然后返回“命令提示符”窗口，使用 diskpart 命令，连接新的“网络”硬盘并为其分配盘符，主要步骤如下。

01 执行 diskpart 命令，如图 12-168 所示。

02 在 diskpart 提示符后，执行 list disk 命令，显示当前系统安装的磁盘，如图 12-169 所示。从列表中可以看到，当前计算机有 2 个磁盘，其中“磁盘 0”是原来计算机上的本地硬盘，而“磁盘 1”是新增加的磁盘，这个硬盘的分区大小是 39GB。



图 12-168 执行 diskpart



图 12-169 显示所有磁盘

03 执行 select disk 1 命令，选择“磁盘 1”作为当前的磁盘，如图 12-170 所示。

04 执行 list partition 命令，显示当前所选磁盘的分区，如图 12-171 所示。当前磁盘有两个分区，其中第 2 个分区大小是 38GB，这是在上一节中，创建动态磁盘后创建的分区。然后执行 select partition 2，选择第 2 个分区。

DISKPART> select disk 1

磁盘 1 现在是所选磁盘。

图 12-170 选择磁盘



图 12-171 显示分区

05 执行 assign letter=p，为选择的分区分配盘符。本例中，分配的盘符为 p，如图 12-172 所示。然后执行 exit 退出 diskpart 命令。

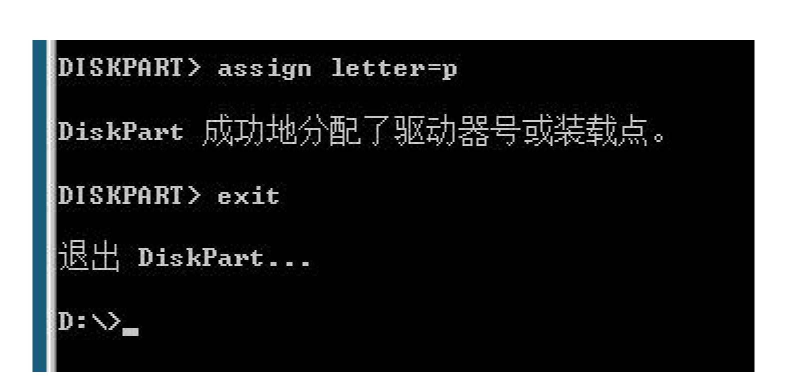


图 12-172 分配盘符

12.5.4 为 Hyper-V 主机添加虚拟机保存路径

在为两台 Hyper-V 主机添加了网络存储之后，还需要在 Hyper-V 进行设置才能供虚拟机使用，主要步骤如下：

01 在 VMM 管理控制台中，在左侧窗格中选择“主机”，并且在“Hyper-V 主机”列表中，选择要进行配置的主机，在右侧的“主机”列表中选择“属性”，如图 12-173 所示。

02 在弹出的对话框中，在“放置”选项卡中单击“添加”按钮，在“选择目标文件夹”对话框中，选择新添加的网络存储磁盘，在本例中为 P 盘，如图 12-174 所示。

对于另一台主机，也要进行添加，在此不再介绍。

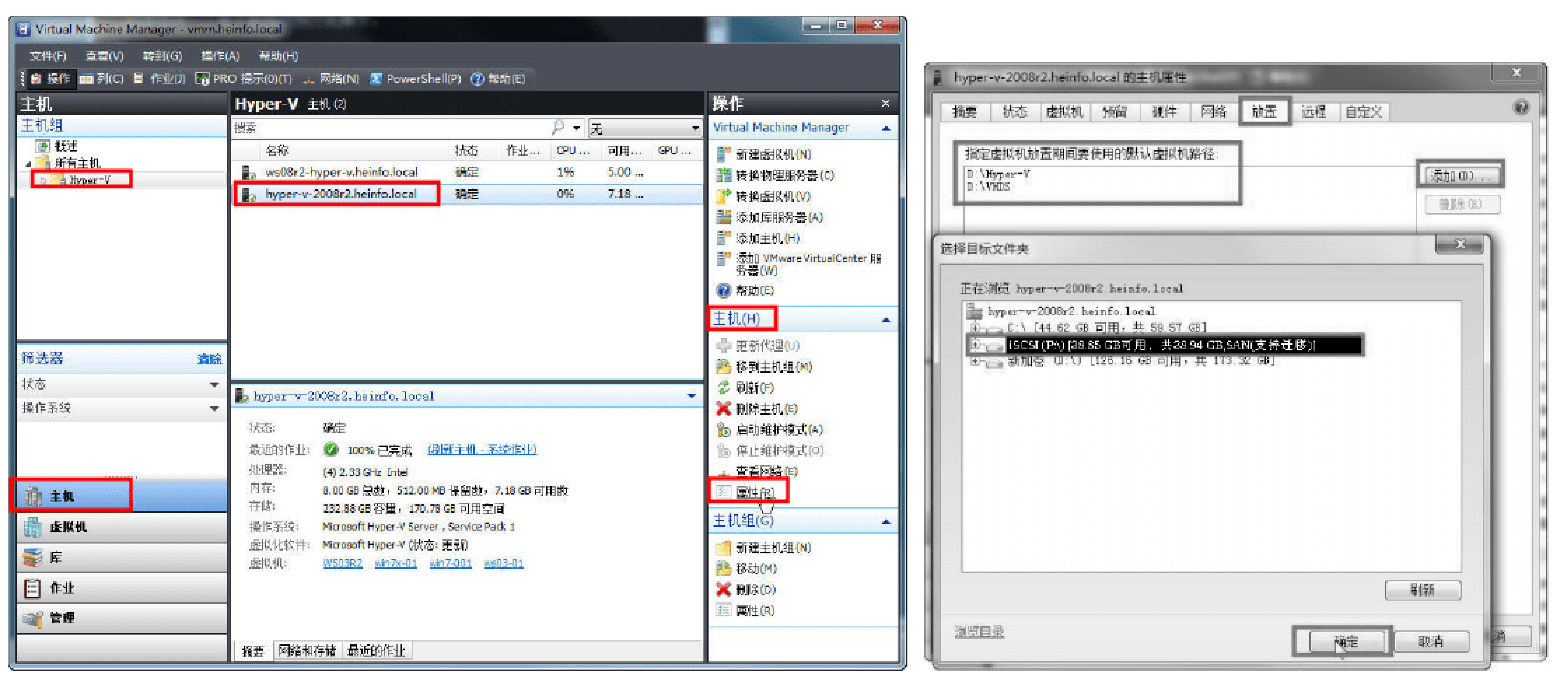


图 12-173　属性　　　　图 12-174　添加虚拟机保存路径

12.5.5　同一主机迁移虚拟机（迁移存储）

在本次操作中，我们介绍在同一主机、不同存储之间迁移虚拟机的方法，步骤如下。

01 在 VMM 管理控制台中，在左侧任务窗格中选择“虚拟机→所有主机→Hyper-V”，从中选择一个主机，在右侧的虚拟机列表中，选择一个准备迁移的虚拟机，用鼠标右击，在弹出的快捷菜单中选择“迁移存储”命令，如图 12-175 所示。

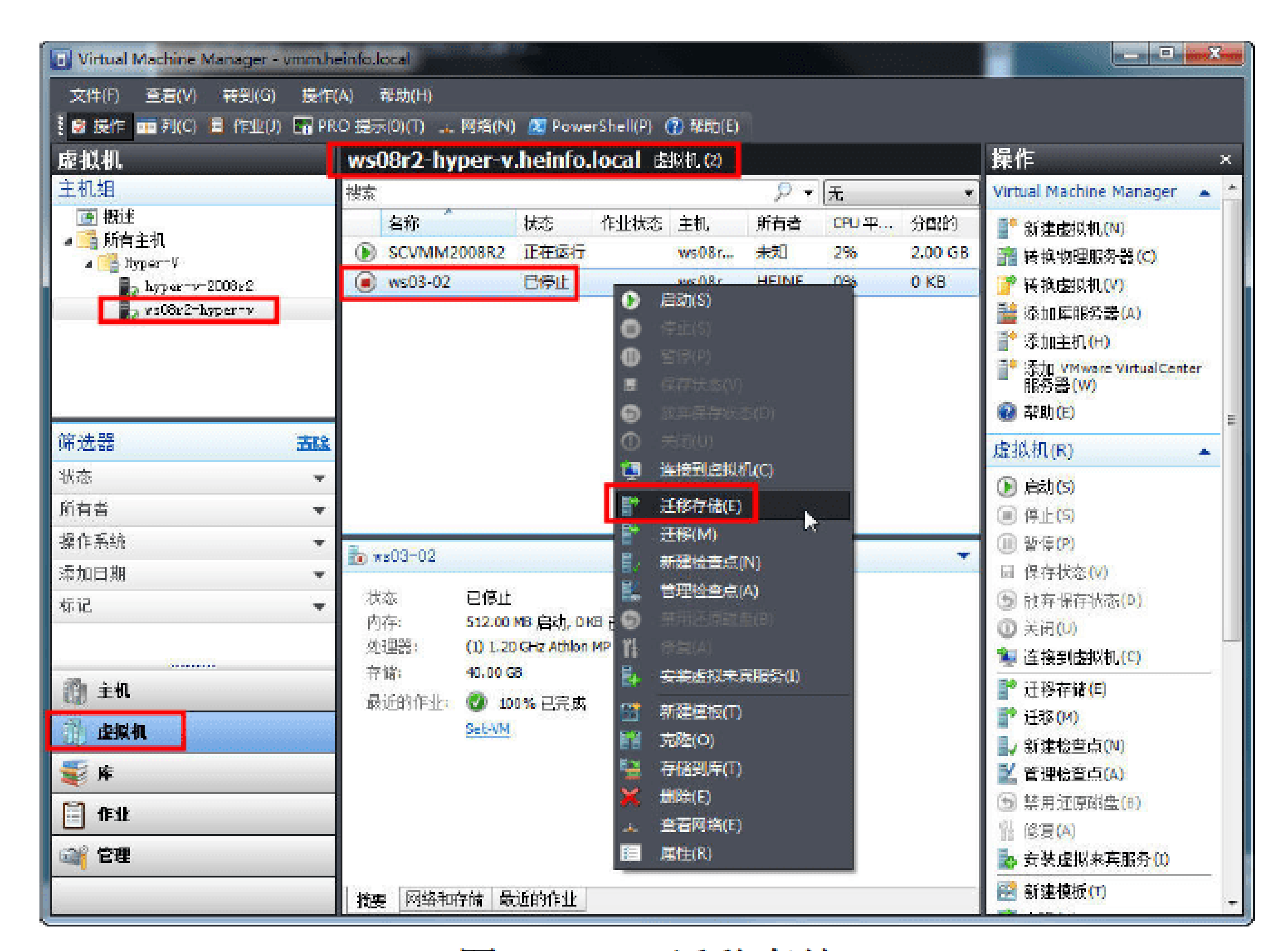


图 12-175　迁移存储

02 在“选择路径”对话框的“虚拟机路径”中，选择新的存储位置。在本例中，选择网络存储 P 盘，如图 12-176 所示。

03 在“摘要”对话框在，显示了虚拟机选择的主机信息，检查无误之后，单击“移动”按钮，如图 12-177 所示。

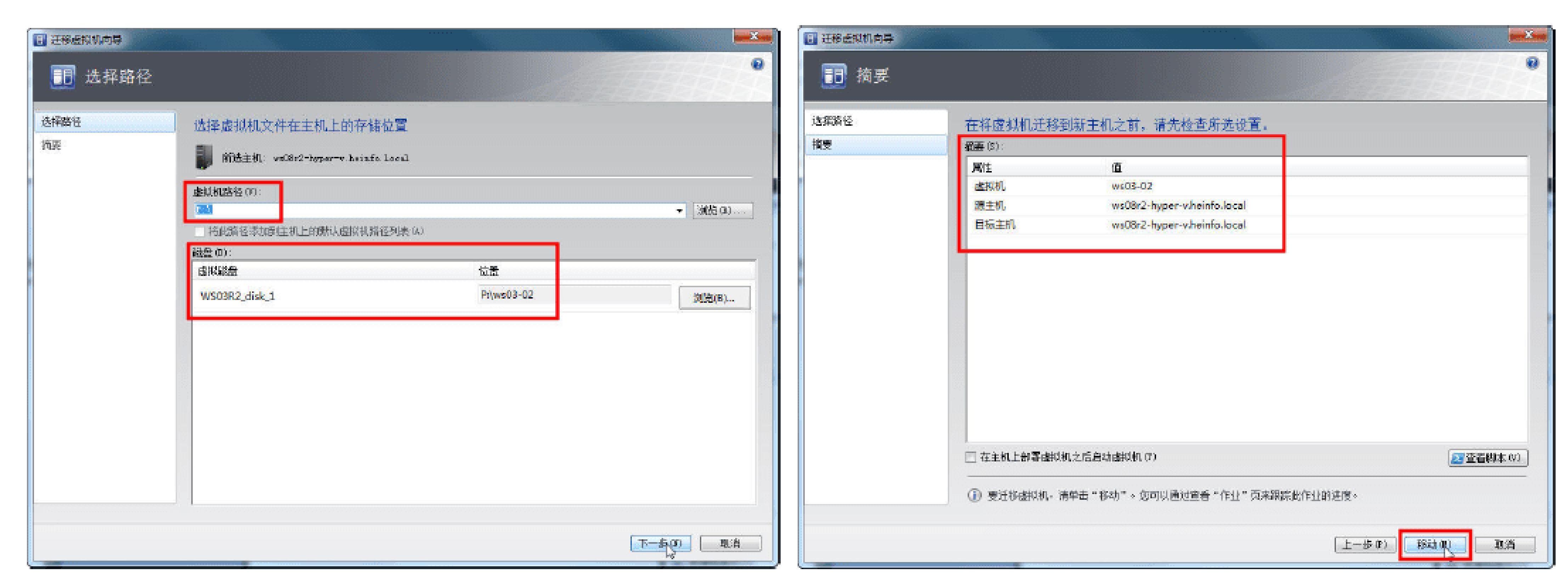


图 12-176 选择路径　　　　图 12-177 摘要

04 然后弹出迁移虚拟机的“作业”窗口，开始迁移虚拟机。迁移的时间视要迁移的虚拟机的磁盘大小、源存储、目标存储的速度而定，在本次迁移中，使用了 1 分 23 秒。迁移完成之后，关闭作业窗口，如图 12-178 所示。

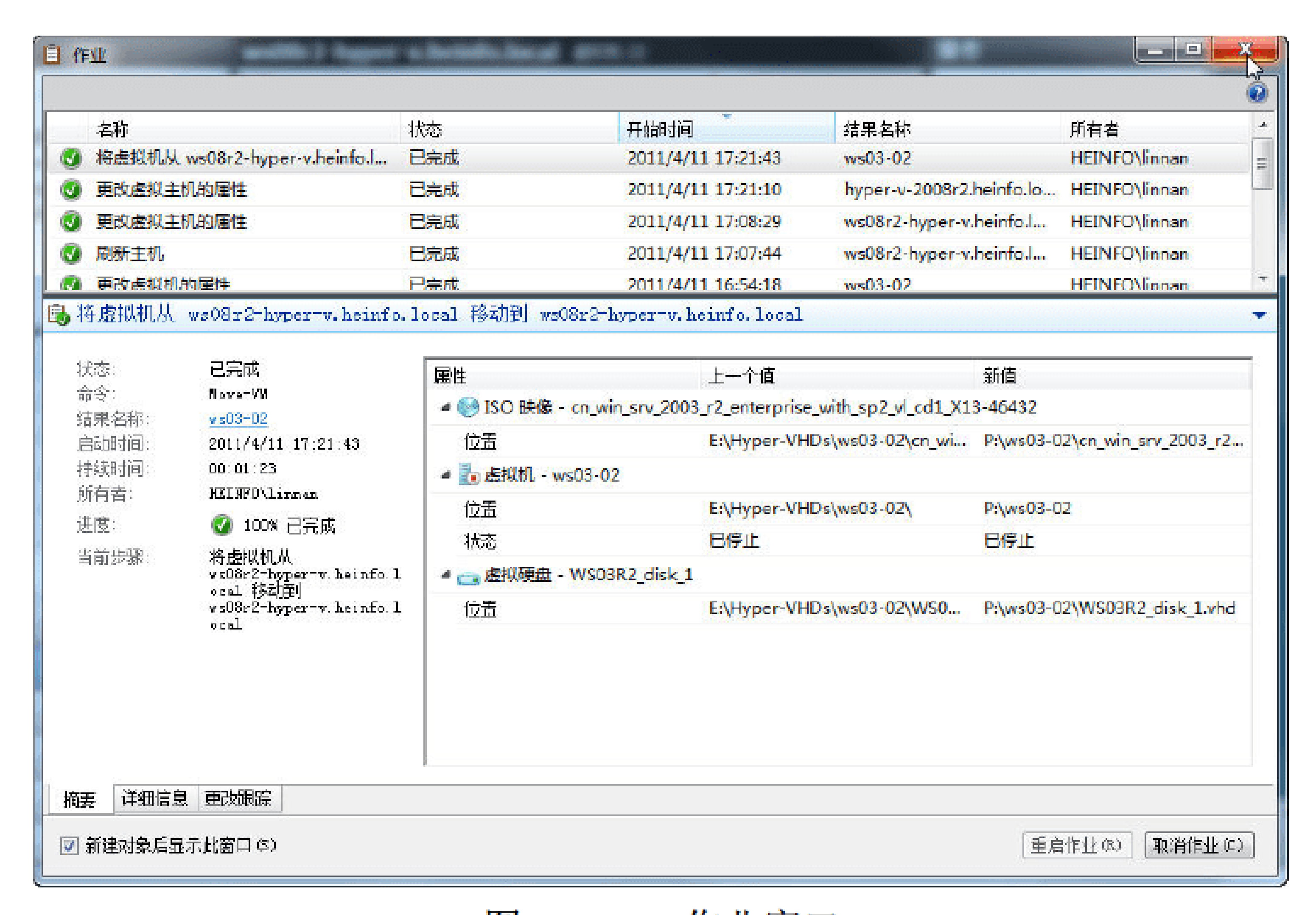


图 12-178 作业窗口

12.5.6 在不同主机间迁移虚拟机

最后，介绍在不同主机之间迁移虚拟机的方法，步骤如下：

01 在 VMM 管理员控制台中，选中一台要迁移的主机，用鼠标右击，在弹出的快捷菜单中选择“迁移”命令，如图 12-179 所示。

02 在“选择主机”对话框中选择另一台主机，如图 12-180 所示。

03 在“选择路径”对话框中选择在目标主机上，虚拟机的保存位置，如图 12-181 所示。

04 在“选择网络”对话框中指定用于虚拟机的虚拟网络，如图 12-182 所示。

05 在“摘要”对话框中显示了迁移的信息，无误之后，单击“移动”按钮，如图 12-183 所示。

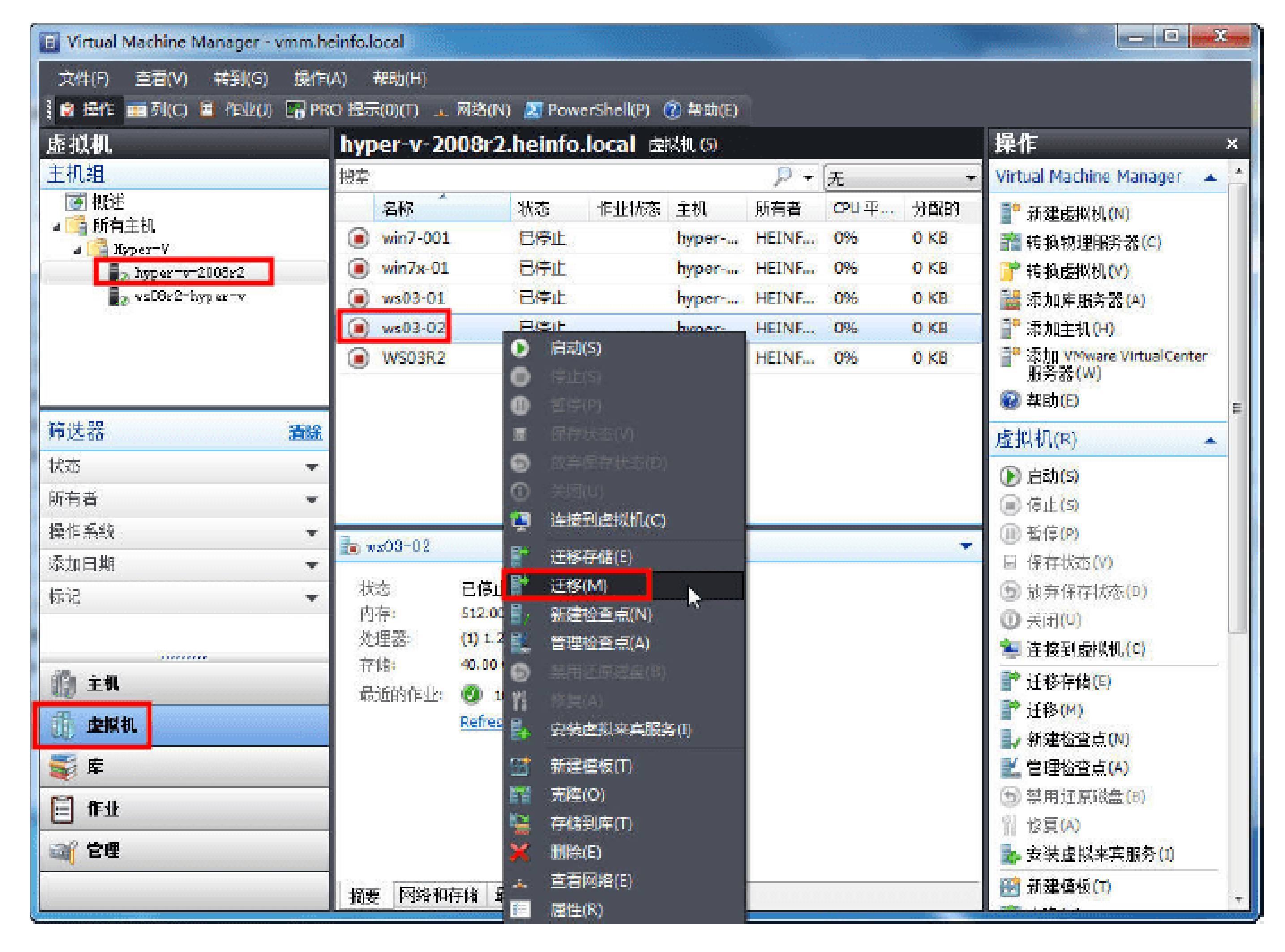


图 12-179　迁移

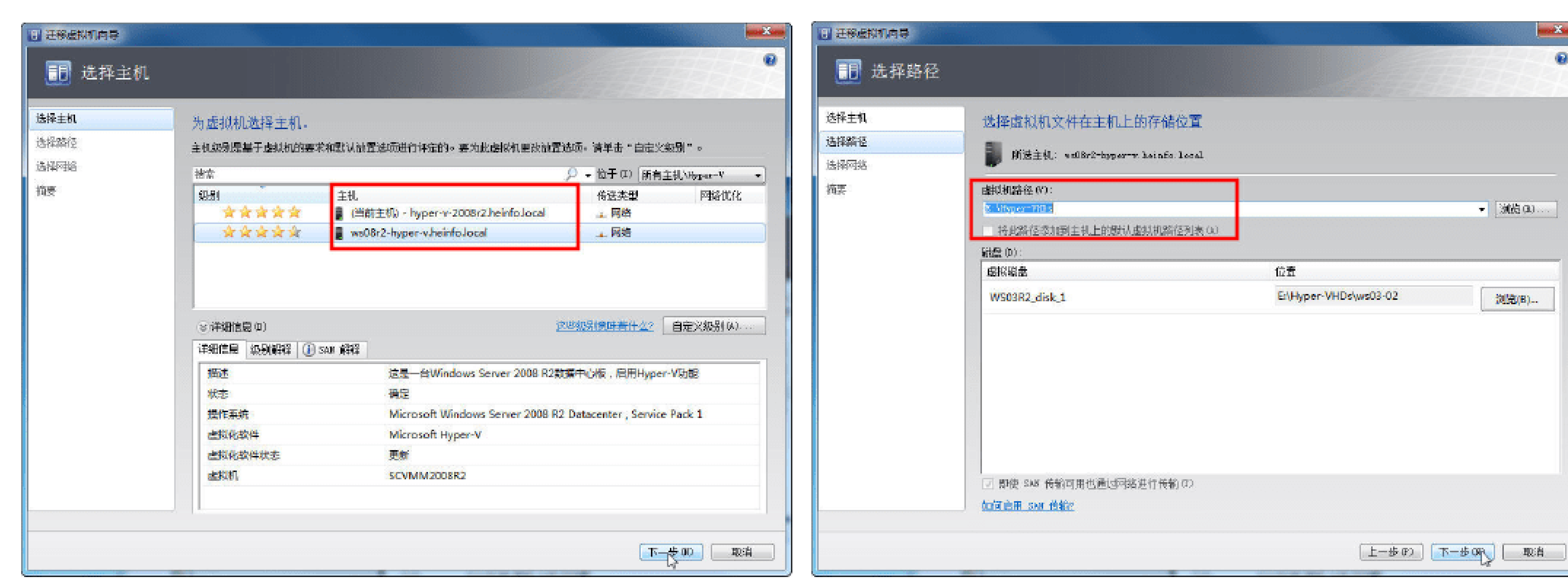


图 12-180　选择另一台主机　　　　　　图 12-181　选择路径

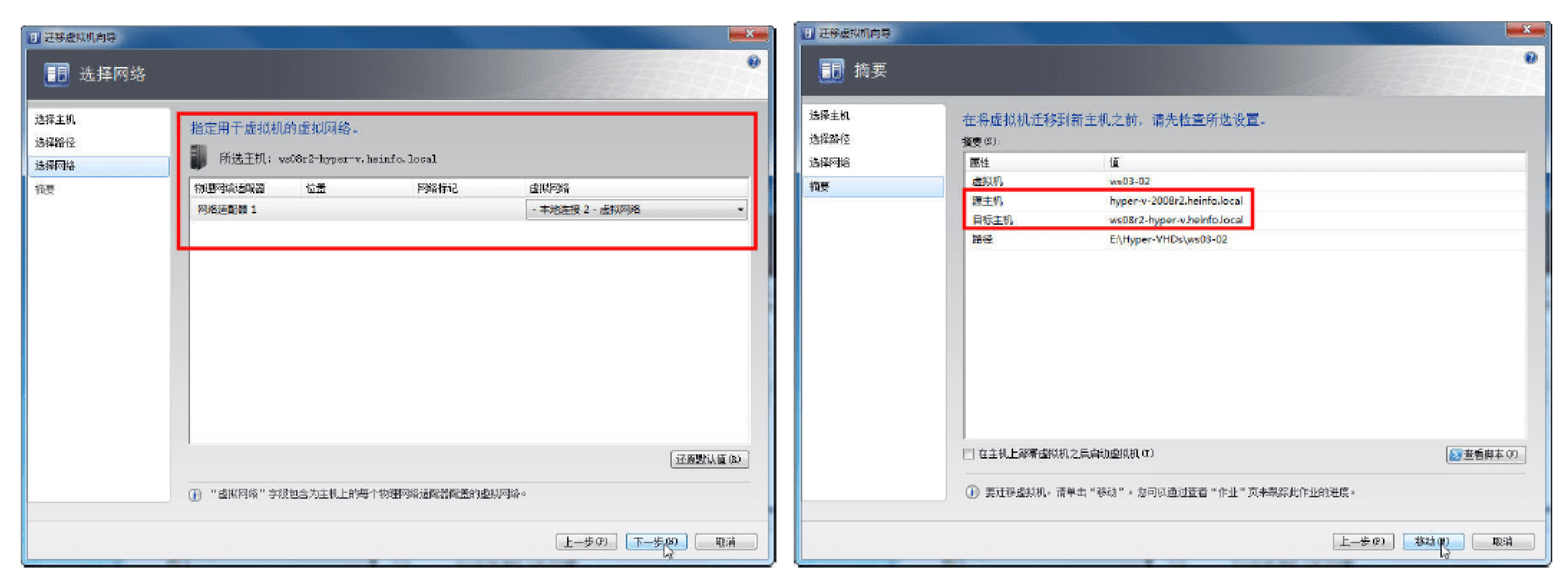


图 12-182　选择网络　　　　　　图 12-183　摘要

06 然后显示“作业”窗口，直到作业完成，如图 12-184 所示。

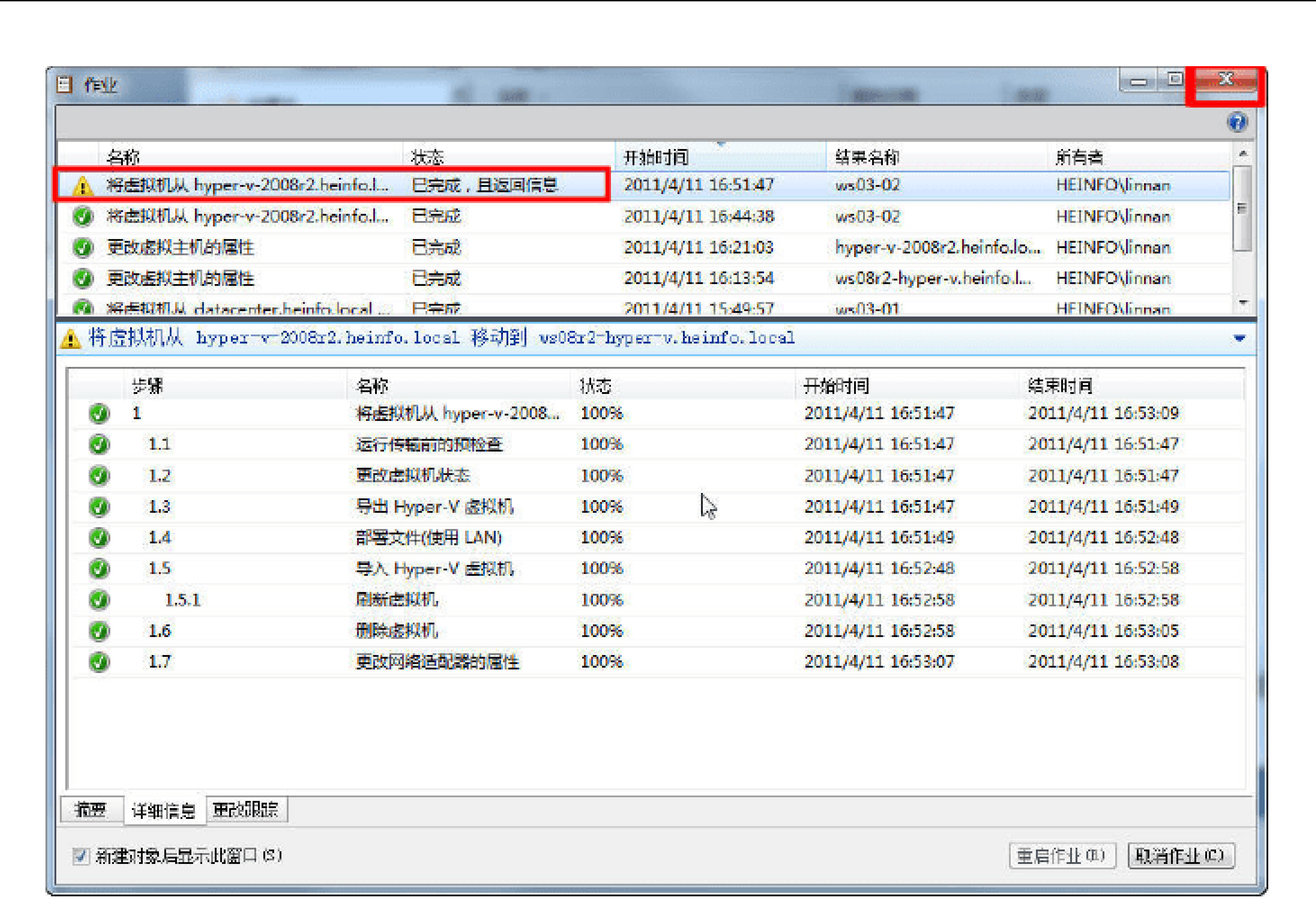


图 12-184　作业窗口

第 13 章　Windows Server 2008 R2 终端虚拟化应用

计算机的更新速度是比较快的，而对计算机的软件需求也是越来越高。3 年之前购置的高配置的机器，在现在看来已经“落伍”了，而现在新购置的机器，在 3 年后肯定也是“淘汰品”。对于个人来说，可能过三四年就会升级配置或更换新的计算机；但对于企业来说，尤其是使用计算机办公的机关、事业单位，如果每三四年更新一批计算机，费用是比较高昂的，但如果不更新又不能满足当前办公软件的需求。

Windows Server 2008 的“终端虚拟化”可以解决这方面的问题，与传统的升级工作站的方式相比，它只需要升级服务器，并且所有的软件都运行在服务器端，而将软件运行的“画面”传送到工作站端，这样，工作站端只需要运行一个极小的软件即可。

13.1　企业网络现状与主要问题

现在政府、机关与事业单位的办公用机大都是 2001 年左右配置的，当时都是 128MB 的、P3 或 P4 的计算机，这些计算机在当时可以很好地运行 Windows 2000 或 Windows XP 操作系统，也可以运行当时的办公软件。但现在的办公软件需要更大的内存、更高的处理器速度以及更大的硬盘。而使用 2001 年、2002，甚至 2006 年流行配置的计算机，运行现在的办公软件，速度是非常缓慢的。

对于许多学校机房来说，由于资金问题，购置的计算机并不是“流行”配置或高配置，而经过几年之后，学生需要学习或练习的都是目前的流行软件，运行这些软件的速度非常慢甚至是不能运行的。

由于现在软件的运行需要更高的配置，导致以前购置的计算机不能使用。传统的方法就是升级工作站的配置，或者淘汰当前的计算机，更换新的计算机，但这样一来，需要的资金是一个比较大的数字。另外，即使现在购置了“高配置”的计算机，但再过几年，仍然要面对工作站的升级问题，这样就走进了“购买→升级→（过几年）落伍→再升级”的怪圈，随着人们对计算机的依赖性越来越高，将来的升级费用也会更高。

实际上，现在的办公计算机都已经“联网”，可以通过网络以及新的产品或技术来解决这个问题。当工作站的配置不能满足当前软件的需求时，升级工作站是一个方法，如果换一种思路，升级服务器未尝不能解决问题。而 Windows Server 2008 R2 的“终端虚拟化”技术就可以解决“工作站”需要频繁升级的问题。

使用 Windows Server 2008 R2 的“终端虚拟化”技术，只需要在企业网络中的一台（或多台）高配置的服务器上，安装所需要的软件，这些软件都运行在服务器端，工作站在需要的时候连接到服务器，服务器端运行软件并将显示界面返回给工作站端，而工作站端将键盘、鼠标的控制命令通过网络发送到服务器，服务器将运行结果再返回给工作站。这样，工作站端只是服务器的一个“终端”，对工作站的要求很低。

13.2 终端虚拟化概述

通过远程桌面服务，可以随时随地为用户提供通过 Internet 或 Intranet 访问任何 Windows 设备上标准 Windows 程序的权限。RemoteApp 则可帮助用户配置程序，使用户可以通过远程桌面服务远程访问程序，就如同最终用户在本地计算机上运行这些程序一样。这些程序称为 RemoteApp 程序。

使用 RemoteApp 管理器可使在远程桌面会话主机（RD 会话主机）服务器上安装的程序，供用户用作 RemoteApp 程序。RemoteApp 管理器会自动安装在已安装 RD 会话主机角色服务的计算机上。

RemoteApp 使您可以通过远程桌面服务远程访问程序，就好像它们在最终用户的本地计算机上运行一样。这些程序称为 RemoteApp 程序。RemoteApp 程序与客户端的桌面集成在一起，而不是在远程桌面会话主机（RD 会话主机）服务器的桌面中向用户显示。RemoteApp 程序在自己的可调整大小的窗口中运行，可以在多个显示器之间拖动，并且在任务栏中有自己的条目。如果用户在同一个 RD 会话主机服务器上运行多个 RemoteApp 程序，则 RemoteApp 程序将共享同一个远程桌面服务会话。

用户可以通过多种方式访问 RemoteApp 程序：

- 使用远程桌面 Web 访问（RD Web 访问）。
- 双击已由管理员创建并分发的远程桌面协议（.rdp）文件。
- 在桌面或“开始”菜单上，双击由管理员使用 Windows Installer（.msi）程序包创建并分发的程序图标。
- 双击文件扩展名与 RemoteApp 程序关联的文件。这可以由管理员使用 Windows Installer 程序包进行配置。

.rdp 文件和 Windows Installer 程序包包含运行 RemoteApp 程序所需的设置。在本地计算机上打开 RemoteApp 程序之后，用户可以与正在 RD 会话主机服务器上运行的该程序进行交互，就好像它们在本地运行一样。

为什么使用 RemoteApp%呢？原因是在许多情况下，RemoteApp 可以降低复杂程度并减少管理开销，包括：

- 分支机构，其本地 IT 支持和网络带宽可能有限。
- 用户需要远程访问程序的情况。

- 部署行业（LOB）程序，尤其是自定义 LOB 程序。
- 没有为用户分配计算机的环境，例如“公用办公桌”或“旅馆式办公”工作区。
- 如果部署某个程序的多个版本，尤其是在本地安装多个版本时，可能会造成冲突。

实际上，RemoteApp 是 Windows 终端服务的“改进”，以前的终端服务，默认是发布整个桌面，包括“开始菜单”“资源管理器”等，即使用户只需要运行终端服务器上的一个程序，也是发布整个桌面（可以修改设置，只运行一个指定的程序）。而在 Windows Server 2008 中，Microsoft 将终端服务进行了扩展，该服务提供了更多、更有实际意义的功能。

由于是采用 RDP 协议访问终端服务器并使用终端服务器提供的应用程序，所以，该种方式对工作站的要求比较低：因为所有的程序都运行在服务器端，工作站端只是显示服务器端运行的程序的结果，并将用户的键盘、鼠标输入反馈到服务器端执行相应的操作，服务器端将运行结果显示在工作站上。所以，这种方式可以用来升级工作站。本人测试这一产品的目的，也是想用来升级学校两个配置比较低的机房，以用来运行 VS2008、AutoCAD 2005 等大型软件。

作为终端服务的改进，RemoteApp 可以很好地与用户工作站的本地磁盘、打印机进行交互。使用 RemoteApp，可以直接访问用户的磁盘并可以使用用户的打印机，而不像以前的终端服务那样，需要在终端服务器与客户端都安装打印驱动程序。

下面将在 Windows Server 2008 R2 中文版中，实现 RemoteApp 的功能。

13.3　远程桌面服务器的安装与配置

在 Windows Server 2008 R2 中，安装“远程桌面服务”与“RemoteApp”程序，然后在服务器上安装需要的应用程序，最后将安装好的应用程序发布到 Web 服务器等提供“资源共享”的地方，而客户端通过访问服务器端的“Web 服务器”或“文件共享”来访问发布的资源，进而连接到服务器，使用运行在服务器端的程序。

13.3.1　在服务器上安装远程桌面

在 Windows Server 2008 R2 服务器上，进入“服务器管理器”窗口，单击“添加角色”按钮，安装 IIS 与远程桌面服务，如图 13-1 所示。

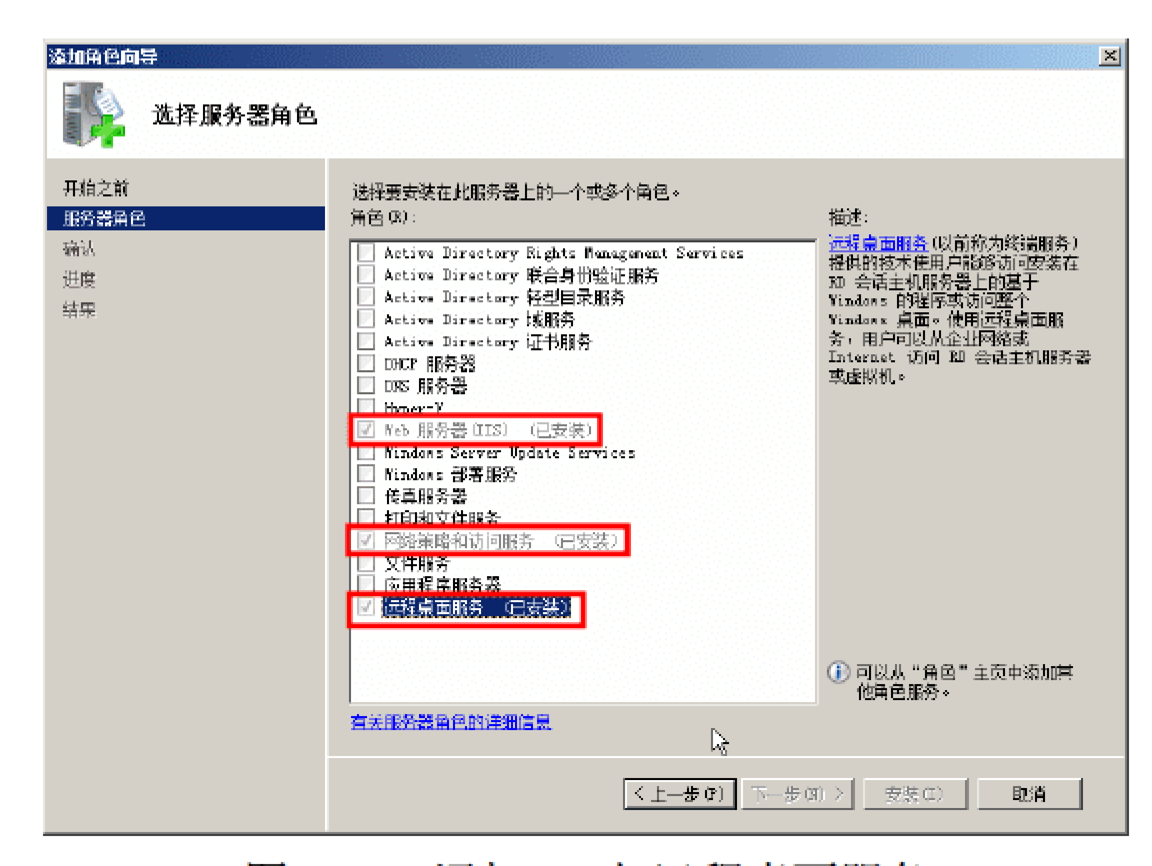


图 13-1　添加 IIS 与远程桌面服务

安装服务之后，重新启动计算机。

13.3.2　安装用于 RemoteApp 的程序

在安装好“远程桌面服务”之后，需要在服务器上，安装 RemoteApp 的程序，主要步骤如下。

01 在服务器中，定位到“控制面板→程序”，如图 13-2 所示。

02 在“程序”窗口中，单击“在远程桌面服务器上安装应用程序”链接，如图 13-3 所示。



图 13-2 添加程序



图 13-3 在远程桌面服务器上安装应用程序

03 插入光盘，浏览选中要安装的程序，这里以安装 AutoCAD 2002 为例，如图 13-4 所示。

04 然后以传统的方法安装程序，如图 13-5 所示。这里使用了一个 AutoCAD 2002 的精简版。



图 13-4 浏览选中安装程序



图 13-5 安装 AutoCAD

05 安装程序完成后，单击“完成”按钮，如图 13-6 所示。

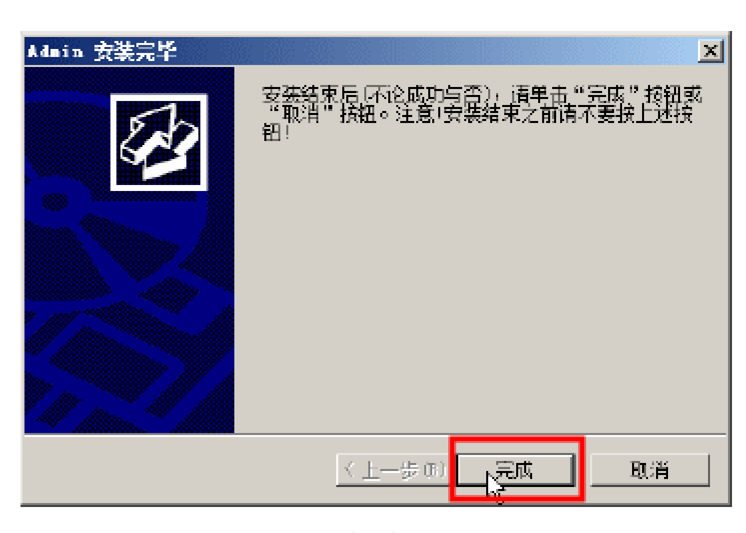
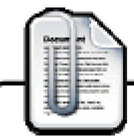


图 13-6 安装程序完成



说 明

每安装一个程序，都要重复图 13-3～图 13-6 的步骤。

06 之后安装其他程序，例如 Office 2007、Photoshop CS、VC、VB、VS2008 等。

13.3.3 添加 RemoteApp

当用于 RemoteApp 的程序安装完成后，返回到“服务器管理器”窗口，定位到“角色→远程桌面服务→RemoteApp 管理器”，单击右侧的“添加 RemoteApp 程序”命令，如图 13-7 所示。

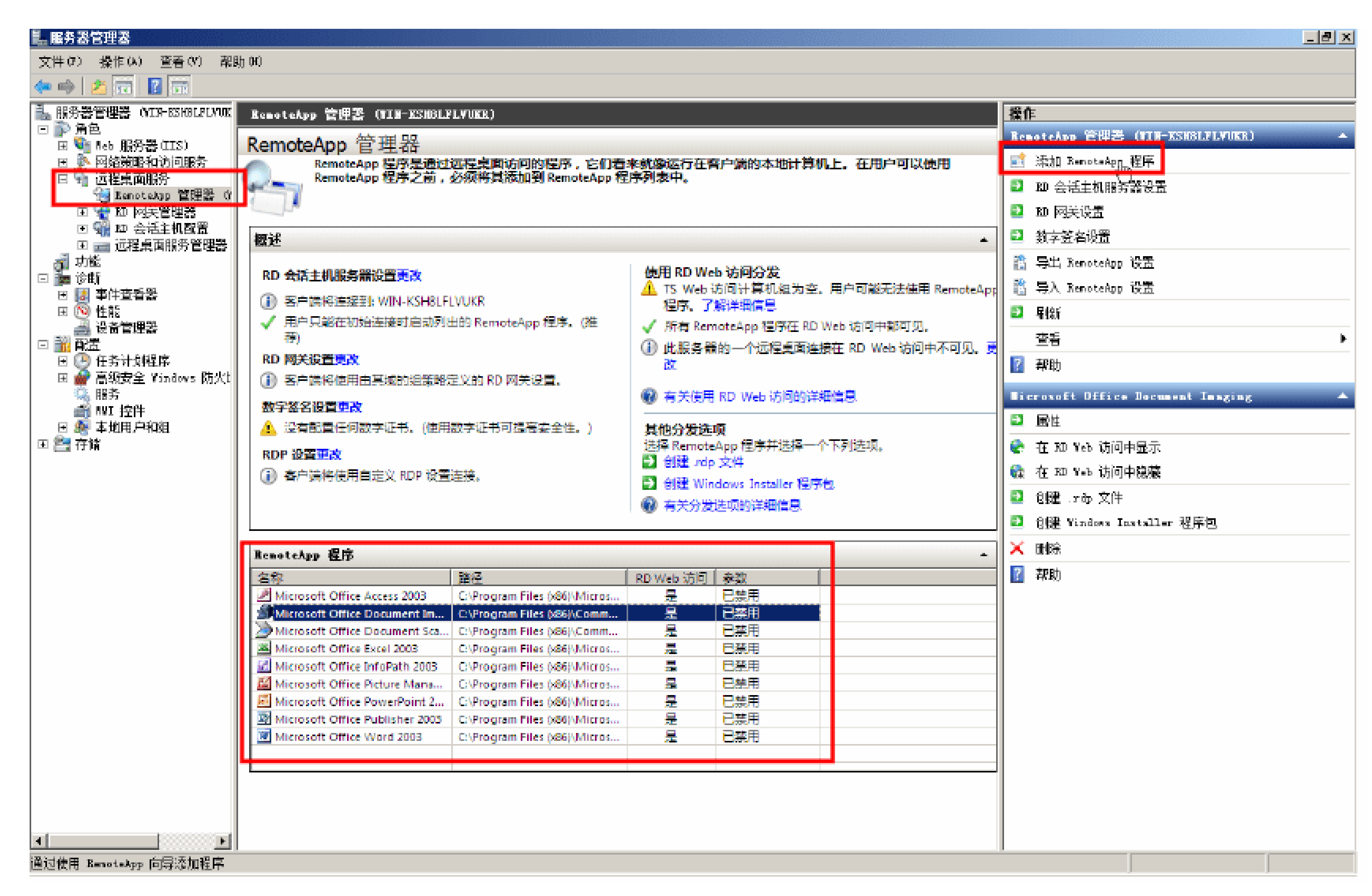


图 13-7 添加 RemoteApp 程序

在“RemoteApp 向导”对话框的“名称”列表中，选择用来添加的 RemoteApp 程序，只需要在前面打上“√”即可，如图 13-8 所示。可以一次选中多个要添加的程序，也可以一次选中一个。

在“复查设置”对话框中，单击“完成”按钮，如图 13-9 所示。

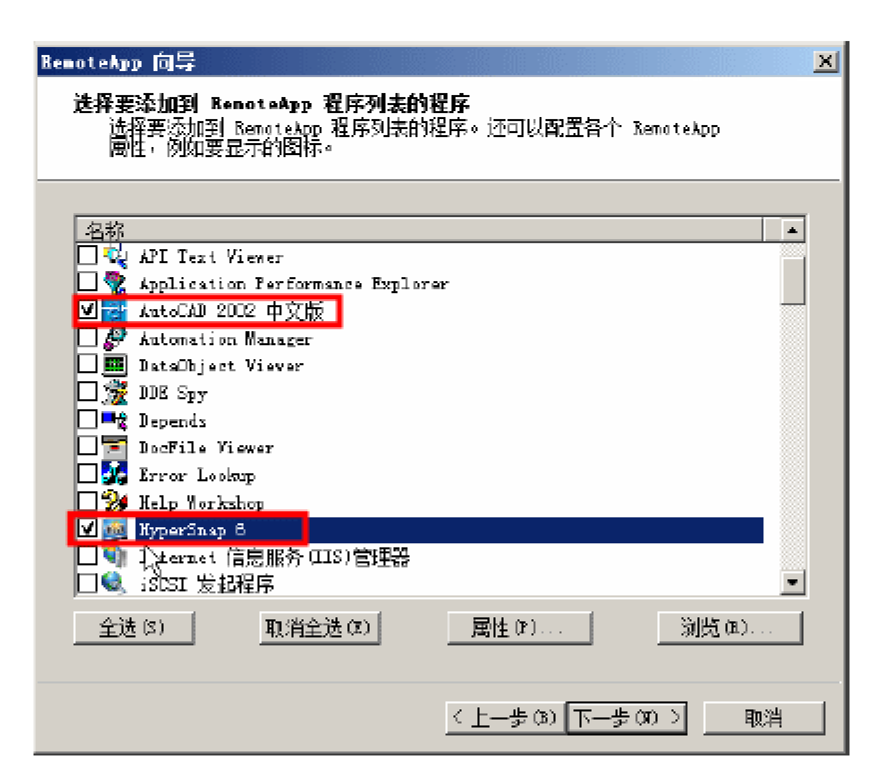


图 13-8 选中要添加的程序

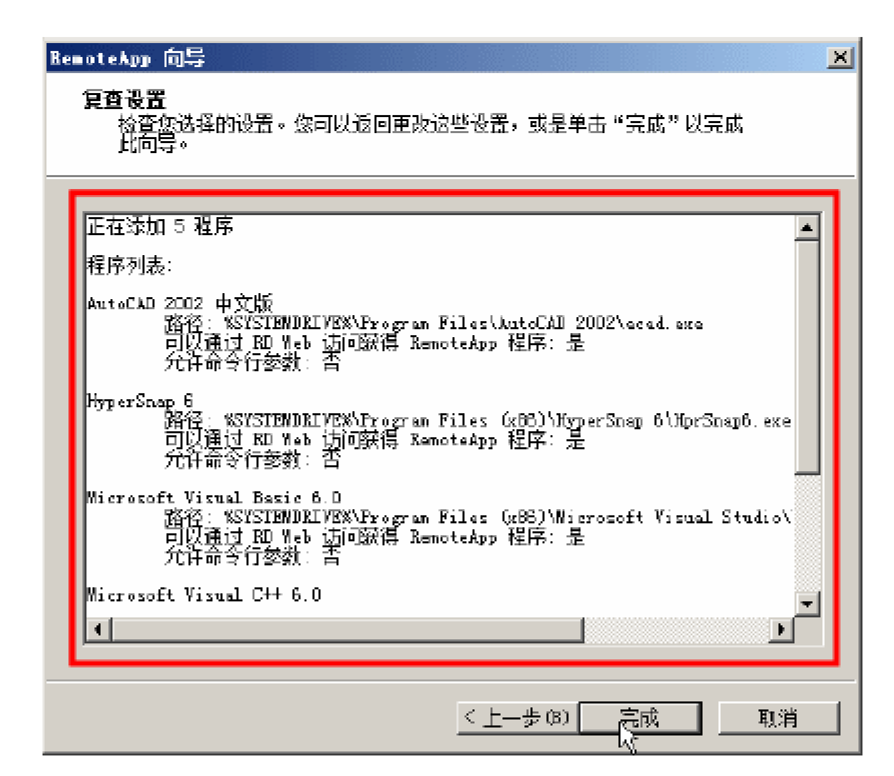


图 13-9 添加程序完成

13.3.4 创建 RDP 文件

在添加 RemoteApp 程序之后，可以将应用程序“发布”，这样就可以在工作站端使用了。首先可以将应用程序发布成“RDP 文件”供工作站端使用。

01 在“服务器管理器”窗口中，定位到在“服务器管理器→远程桌面服务→RemoteApp 管理器”，在“其他分发选项”列表中，单击“创建.rdp 文件”链接，创建客户端使用的 rdp 文件，如图 13-10 所示。

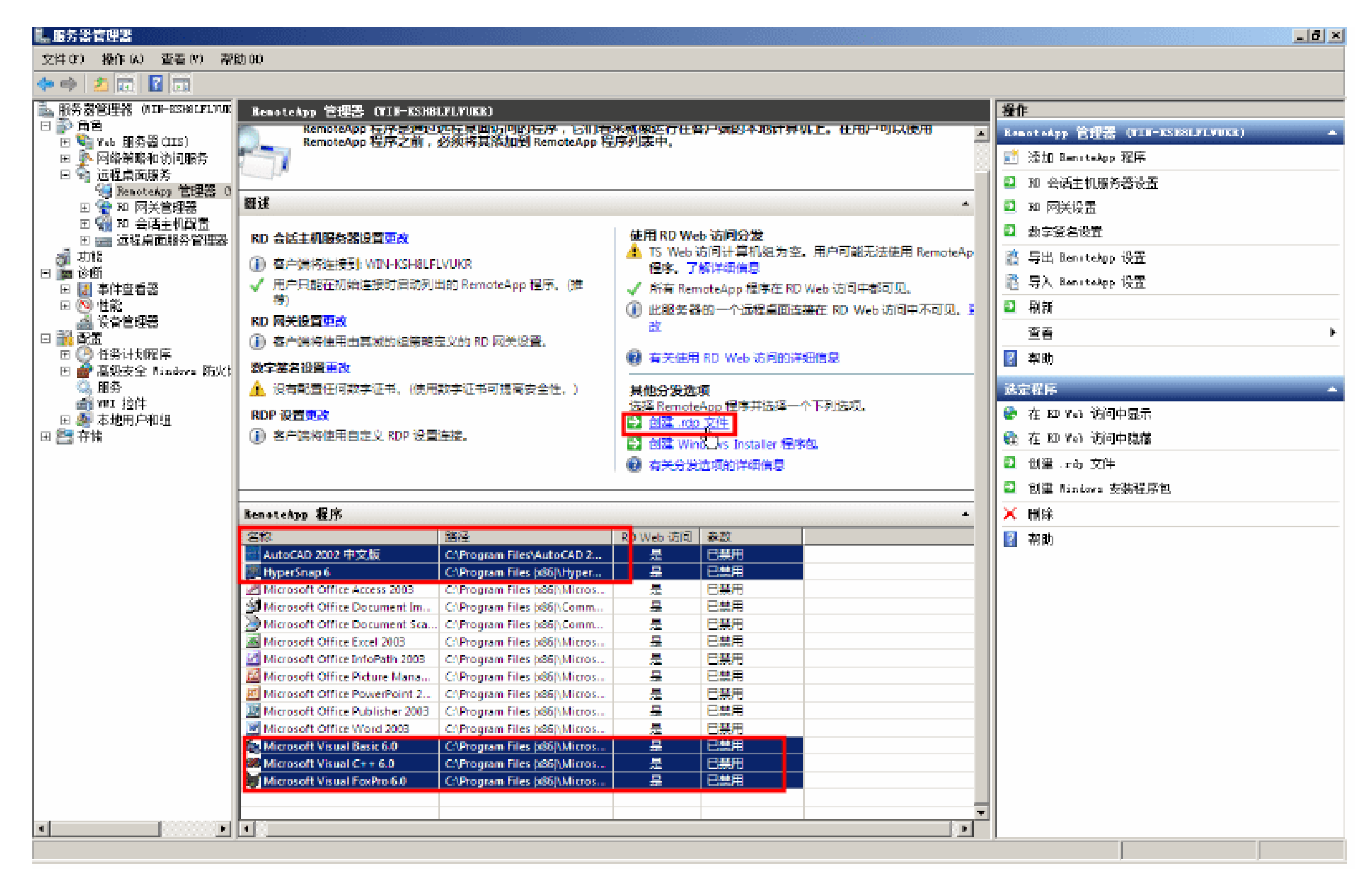


图 13-10　创建.rdp 文件

02 在“欢迎使用 RemoteApp 向导”对话框中，单击“下一步”按钮，如图 13-11 所示。

03 在“指定程序包设置”对话框中，设置.rdp 文件保存路径 、服务器名称等，一般默认保存路径（C:\Program Files\Packaged Programs）即可，如图 13-12 所示。

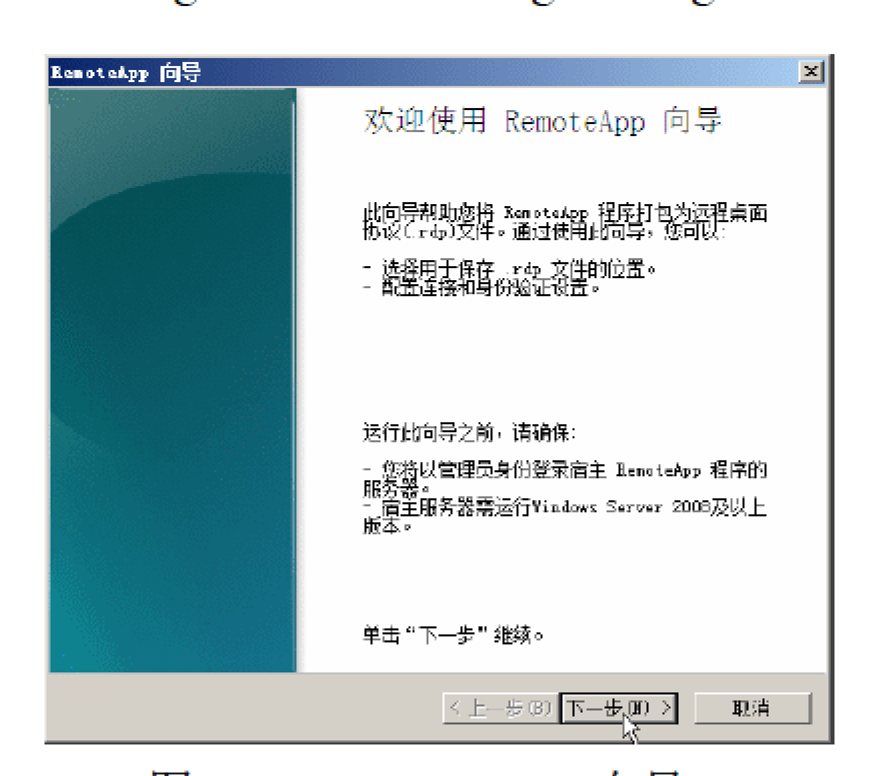


图 13-11　RemoteApp 向导

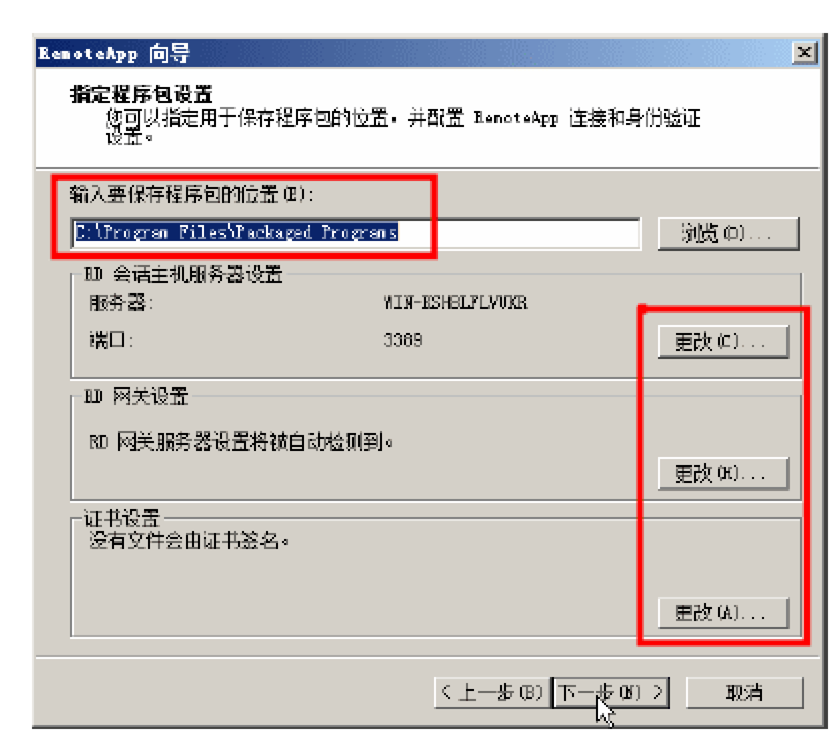


图 13-12　指定程序包位置

04 在“复查设置”对话框中，单击“完成”按钮，如图 13-13 所示。

05 打开图 13-12 中保存 RDP 文件的文件夹，默认为 C:\Program Files\Packaged Programs 文件夹，可以看到发布的应用程序，如图 13-14 所示。

06 之后，将创建的 rdp 文件复制到客户端，用户双击相应的客户端即可调用服务器上相对应的程序了。

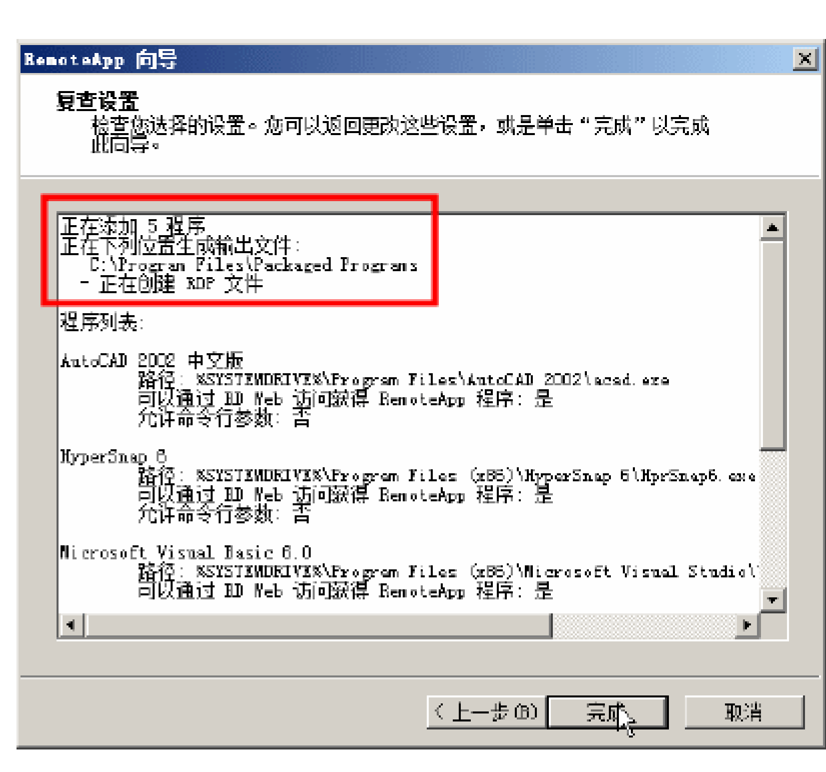


图 13-13　复查设置

图 13-14　发布的应用程序

为了方便客户的使用，可以将图 13-14 中保存 rdp 文件的文件夹设置为共享，如图 13-15 所示。

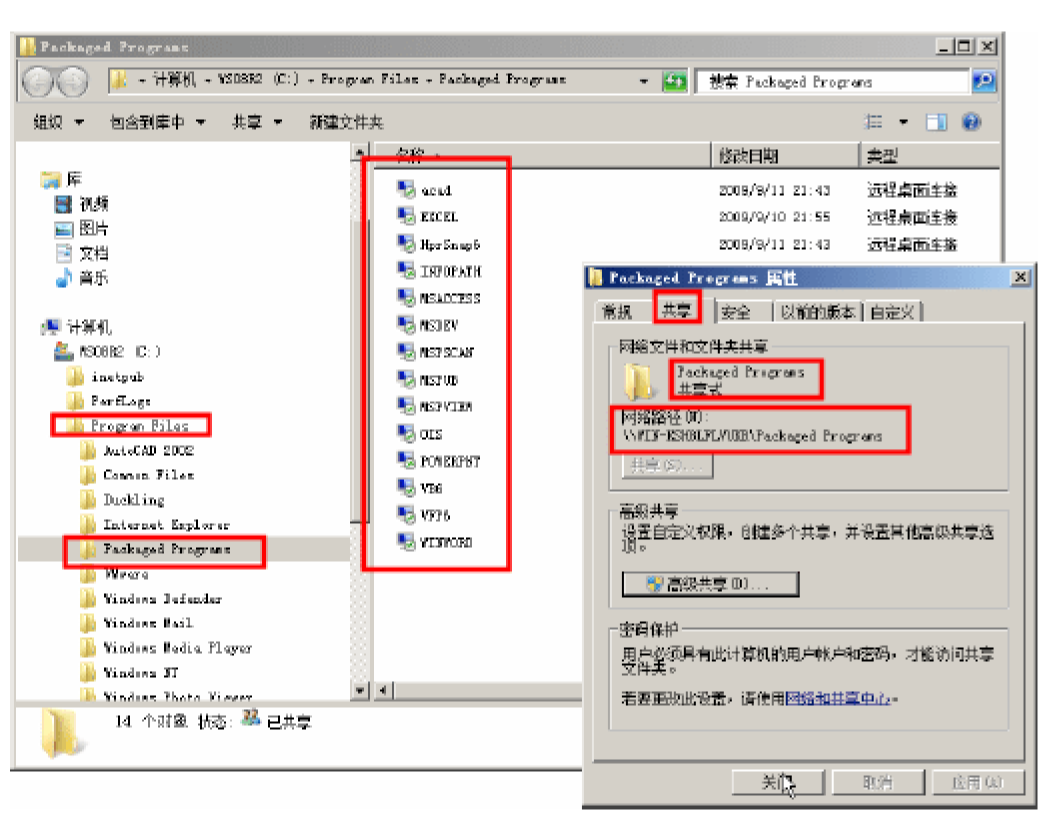


图 13-15　设置为共享

以后在客户端，通过网络共享访问这些 rdp 文件，就可以运行服务器上经过发布的 RemoteApp 程序了。

13.3.5　将 RemoteApp 程序发布到 Web 页

如果用户认为通过网络共享的方式访问 rdp 文件“麻烦”，还可以将这些程序发布到网站中，供用户浏览选用。这种方法很简单，只要在“RemoteApp 程序”列表中选择要发布的程序，然后单击右侧的“在 RD WEB 访问中显示”即可，如图 13-16 所示。

返回到“服务器管理器→角色→Web 服务器→Internet 信息服务”中可以看到，默认保存发布的 RemoteApp 的 Web 页在名为“RDweb”的虚拟目录中，在工作站中浏览这个网站就可以看到发布的 RemoteApp 应用程序。

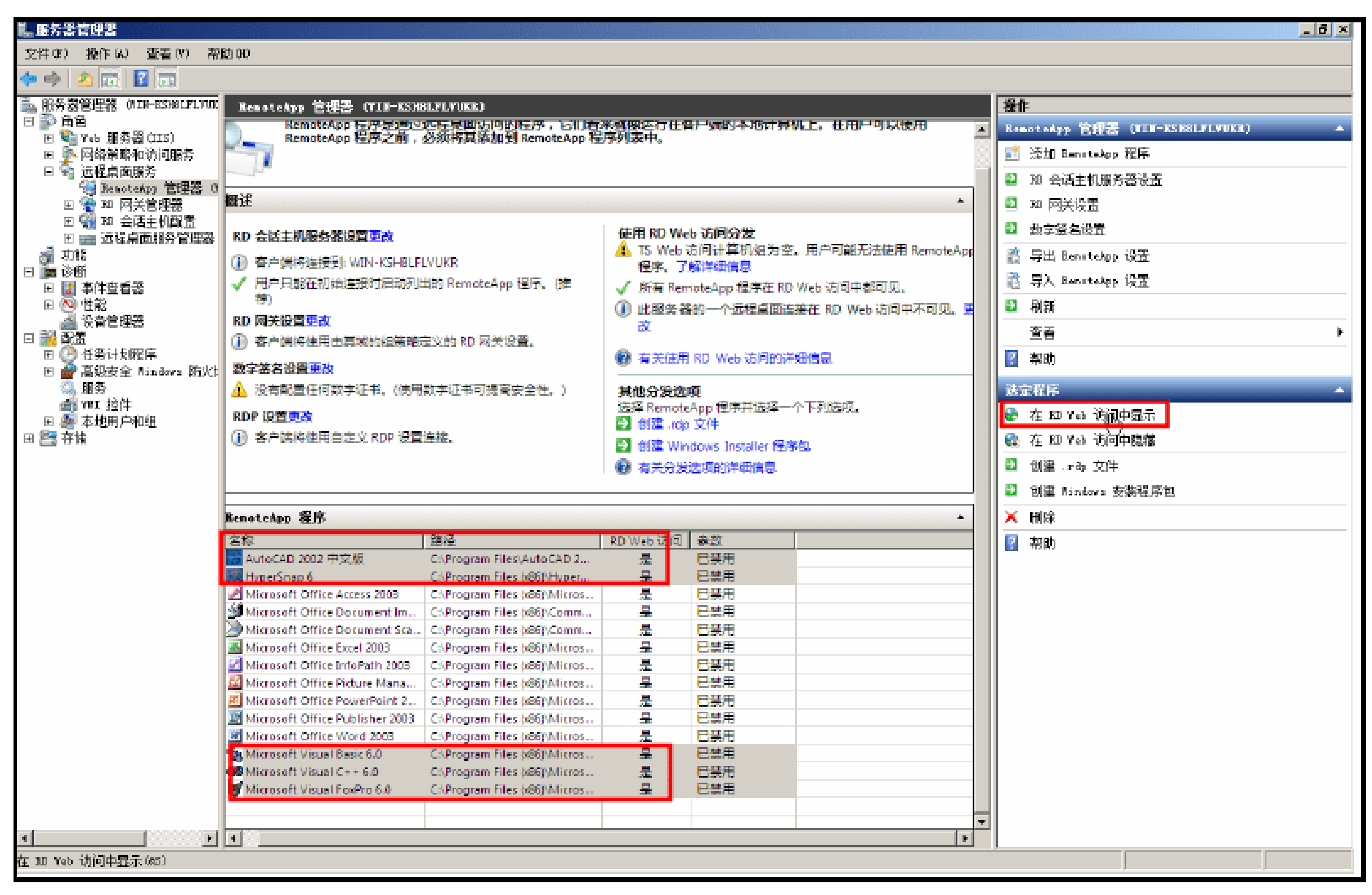


图 13-16　发布到 WEB 页

13.3.6　创建 Windows Installer 程序包

如果想将 RemoteApp 程序“集成”到每个工作站中，可以将 RemoteApp 程序发布成“Windows Installer 程序包”，然后在工作站上运行发布的程序，就可以将服务器端的程序“集成”到工作站端。主要步骤如下。

01 在“服务器管理器→远程桌面服务→RemoteApp 管理器”中，在“RemoteApp 程序”列表中选择要发布的程序，然后单击“创建 Windows Installer 程序包”链接，如图 13-17 所示。

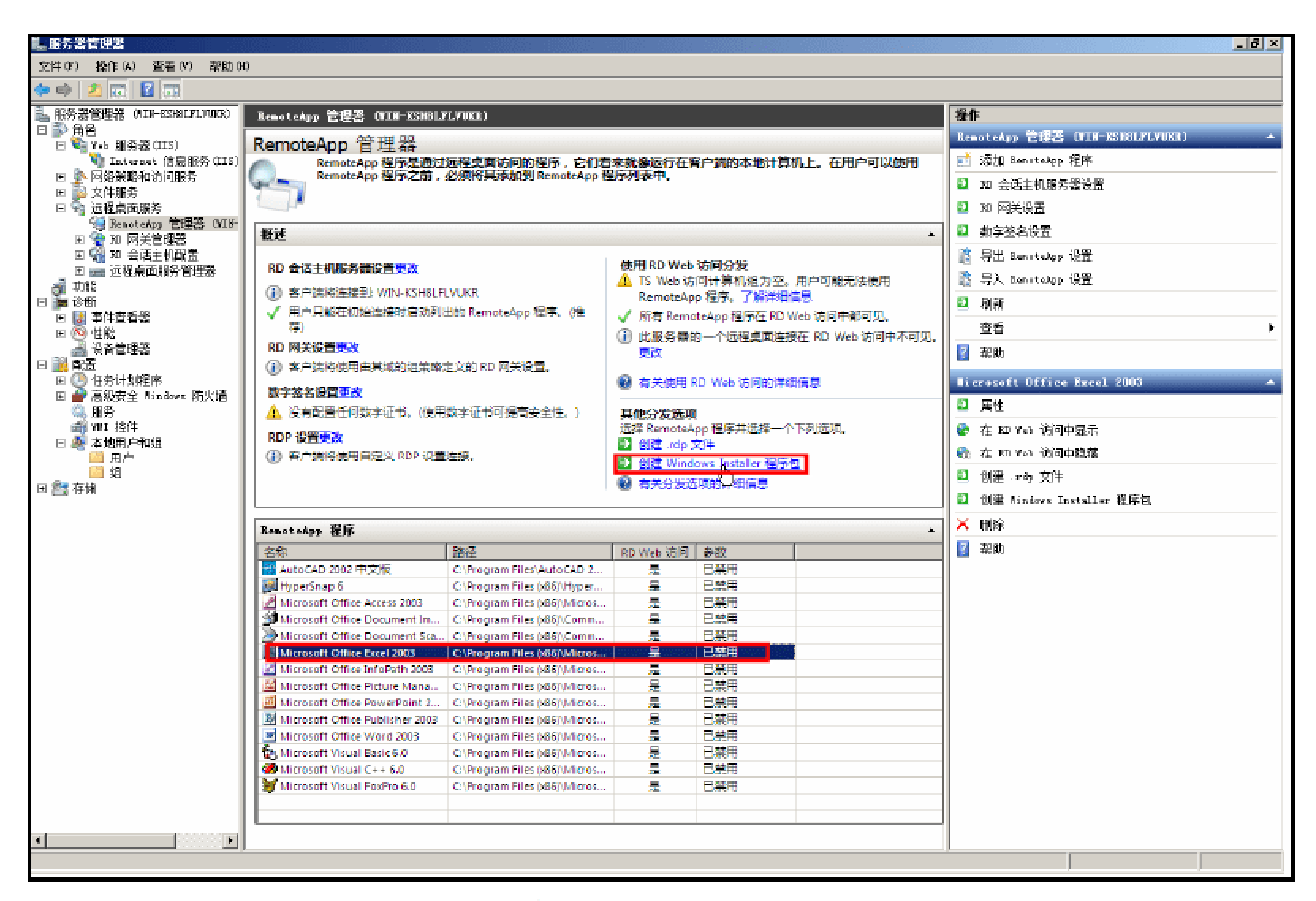


图 13-17　发布 Windows Install 程序包

02 在“欢迎使用 RemoteApp 向导”对话框中，单击“下一步”按钮，如图 13-18 所示。

03 在“指定程序包设置”对话框中，选择要发布的程序包的位置，默认与发布的 RDP 文件

保存在同一文件夹，如图 13-19 所示。

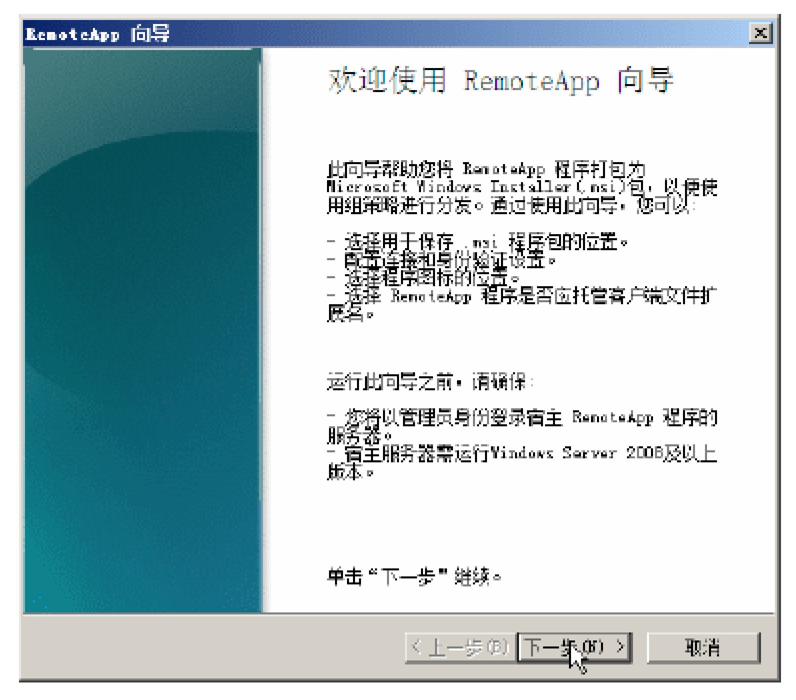


图 13-18　向导



图 13-19　指定程序要保存的位置

04 在“配置发布程序包”对话框中，设置“快捷方式图标”。例如，可以将程序发布到工作站的“桌面”或“开始菜单”，如图 13-20 所示。

05 在“复查设置”对话框中，单击“完成”按钮，完成 Windows Installer 程序包的发布，如图 13-21 所示。

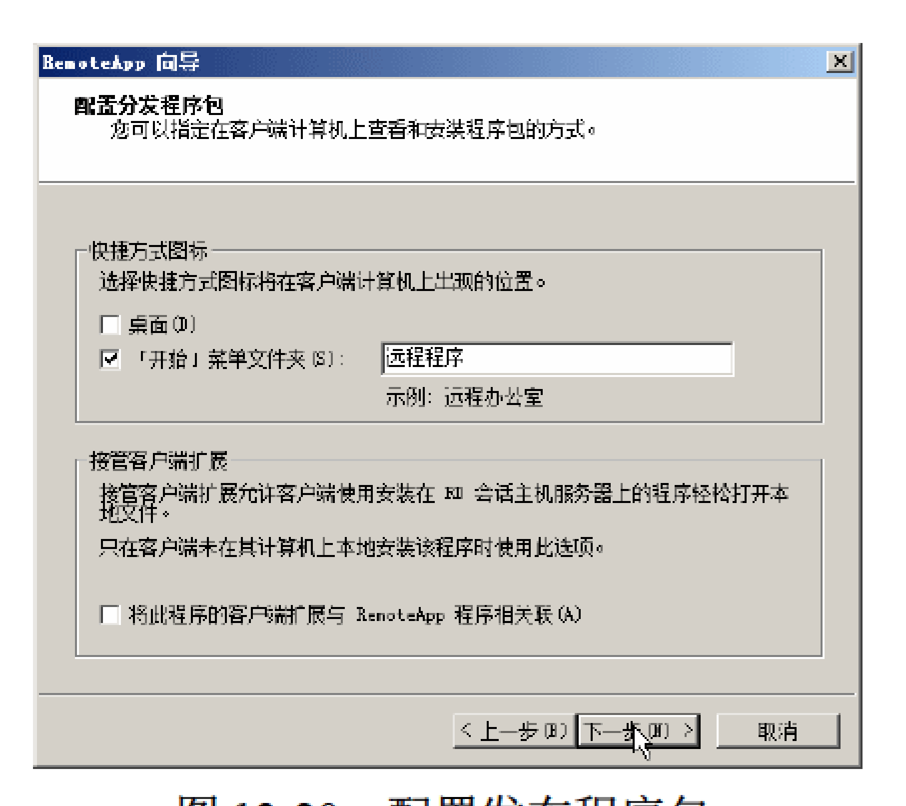


图 13-20　配置发布程序包

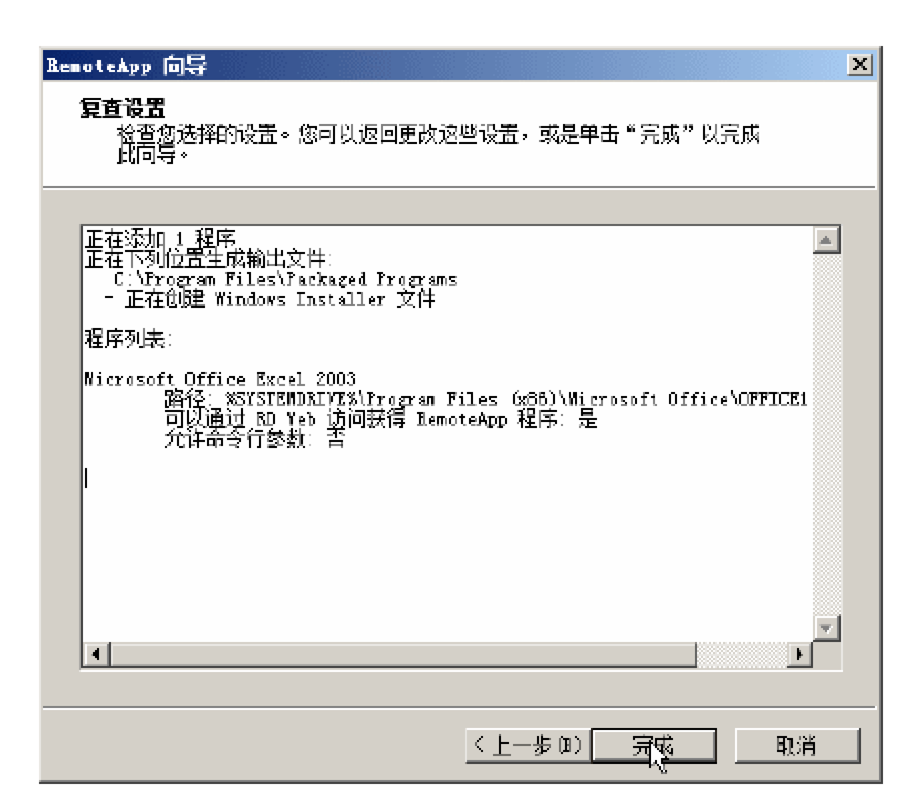


图 13-21　复查设置

06 客户端使用：可以将上面发布的 Windows Installer 的程序包，以“组策略”发布软件的方式，让工作站自动安装；也可以以“共享文件夹”的方式，让工作站连接到服务器安装；或者通过其他共享方式，让工作站运行发布的 Windows Installer 程序。这样，发布的程序将“附加”在工作站的“所有程序→远程程序”文件夹中，如图 13-22 所示。



图 13-22　发布的程序

之后，就可以在工作站端的“远程程序”中（或桌面上，这要看图 13-20 的设置），使用发布的程序了。

13.4　在工作站端测试 RemoteApp 程序

可以通过 Web 站点、RDP 文件和 Windows Installer 程序包 3 种方式，来访问服务器发布的 RemoteApp 程序，下面分别介绍。

13.4.1　通过 Web 站点访问服务器提供的 RemoteApp 程序

首先介绍通过 Web 站点访问服务器提供的 RemoteApp 程序，主要操作步骤如下。

01 在服务器端发布程序时，是以“NetBios 名称”发布的，所以，在工作站访问时，还必须以 NetBios 名称访问服务器。当服务器不是域服务器并且使用 NetBIOS 名称时，需要编辑工作站的 hosts 文件，解析服务器的名称到相应的 IP 地址，如图 13-23 所示。

02 然后打开 IE 浏览器，输入 http://服务器名称/rdweb，如果是 IE7 或 IE8，则需要单击“继续浏览此网站”链接，如图 13-24 所示。

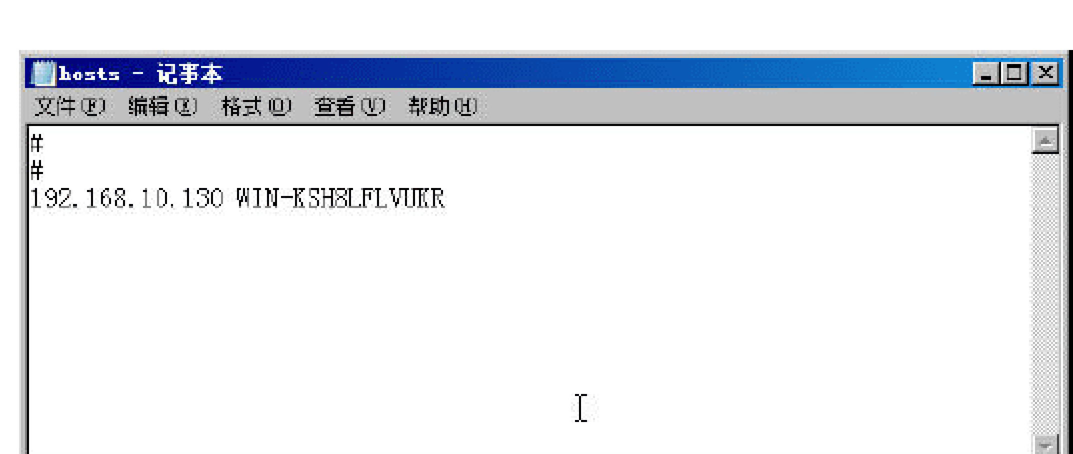


图 13-23　编辑 hosts 文件

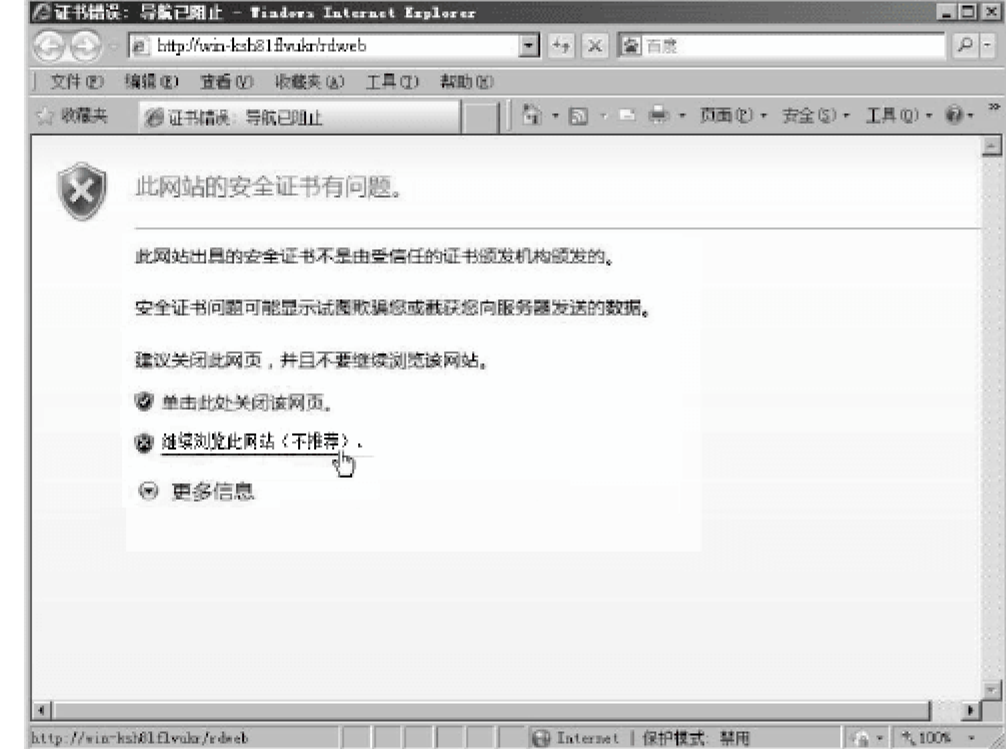


图 13-24　浏览 RemoteApp 服务器

03 输入服务器用户名、密码登录。用户名可以是普通用户，但该用户需要加入到“远程桌面用户组”中，如图 13-25 所示。

04 进入之后，下载并运行 ActiveX 控件，如图 13-26 所示。



图 13-25　登录



图 13-26　运行 ActiveX 控件

05 之后，登录到服务器发布的 Web 页，看到发布的“RemoteApp 程序”与“远程桌面”，如图 13-27 所示。

06 单击某个程序的链接，弹出类似远程桌面的连接设置对话框，在此选中“驱动器”、“打印机”、“剪贴板”等复选框，可以在运行终端服务器的程序时，使用本地的资源，如图 13-28 所示。

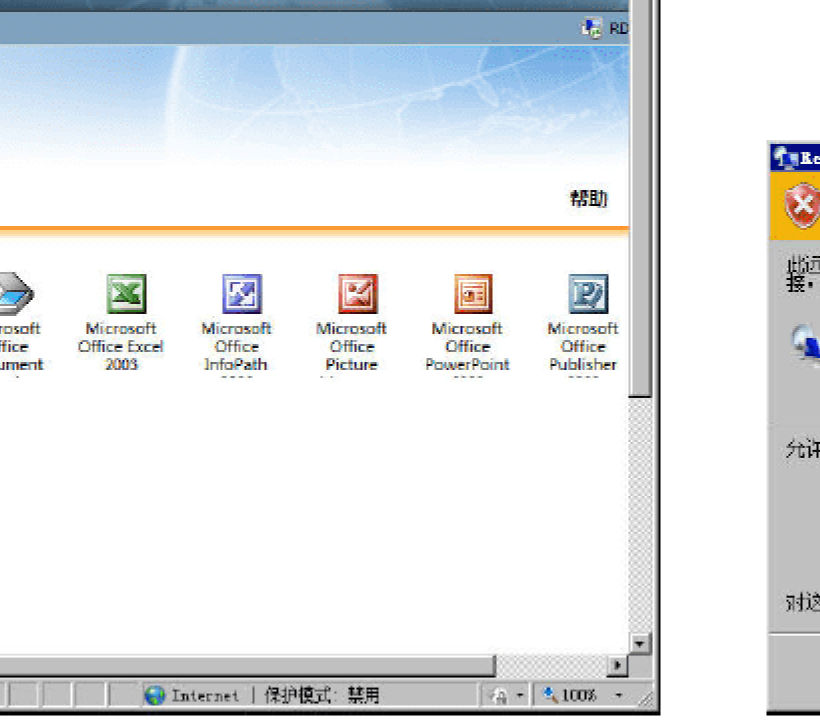



图 13-27　服务器发布的程序

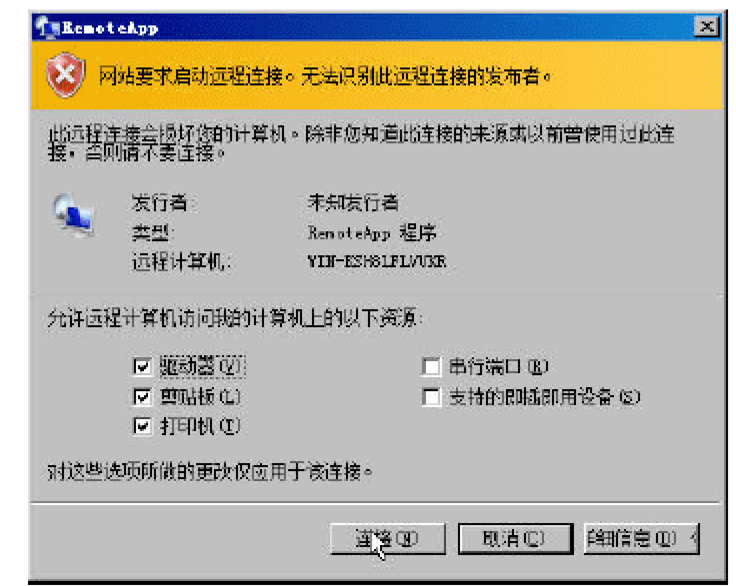


图 13-28　远程桌面客户端连接设置

07 再次输入用户名、密码，这是登录到远程桌面的用户名与密码，如图 13-29 所示。

08 此时将以“远程桌面”的方式启动服务器端的程序，如图 13-30 所示。

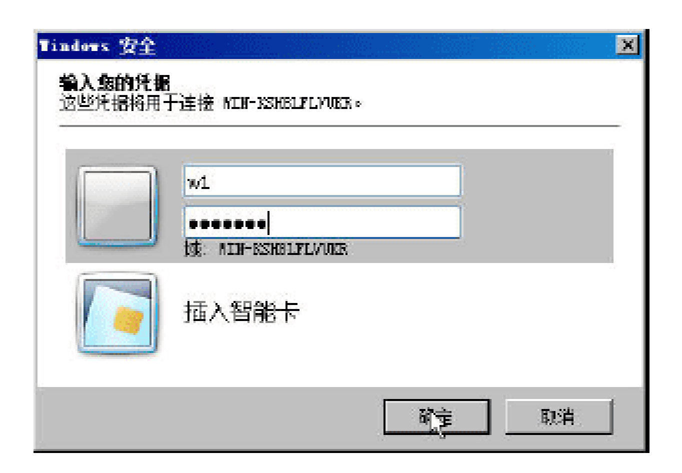


图 13-29　输入服务器用户名与密码



图 13-30　启动程序

09 之后就可以运行程序，如图 13-31 所示，这和在本地计算机上没有明显的区别。

其中“输入法”也是服务器中的输入法，不能使用本地工作站的输入法。

10 图 13-32 是运行服务器上的 AutoCAD 2002 时的界面。

11 如果要打开或保存编辑后的数据，既可以打开（或保存）本机中的文件，也可以使用服务器中的文件。保存/打开本地硬盘数据的截图，如图 13-33 所示。其中 W2008ENT 上的 F 是用户端的 E 盘，W2008ENT 是用户端计算机的名称。

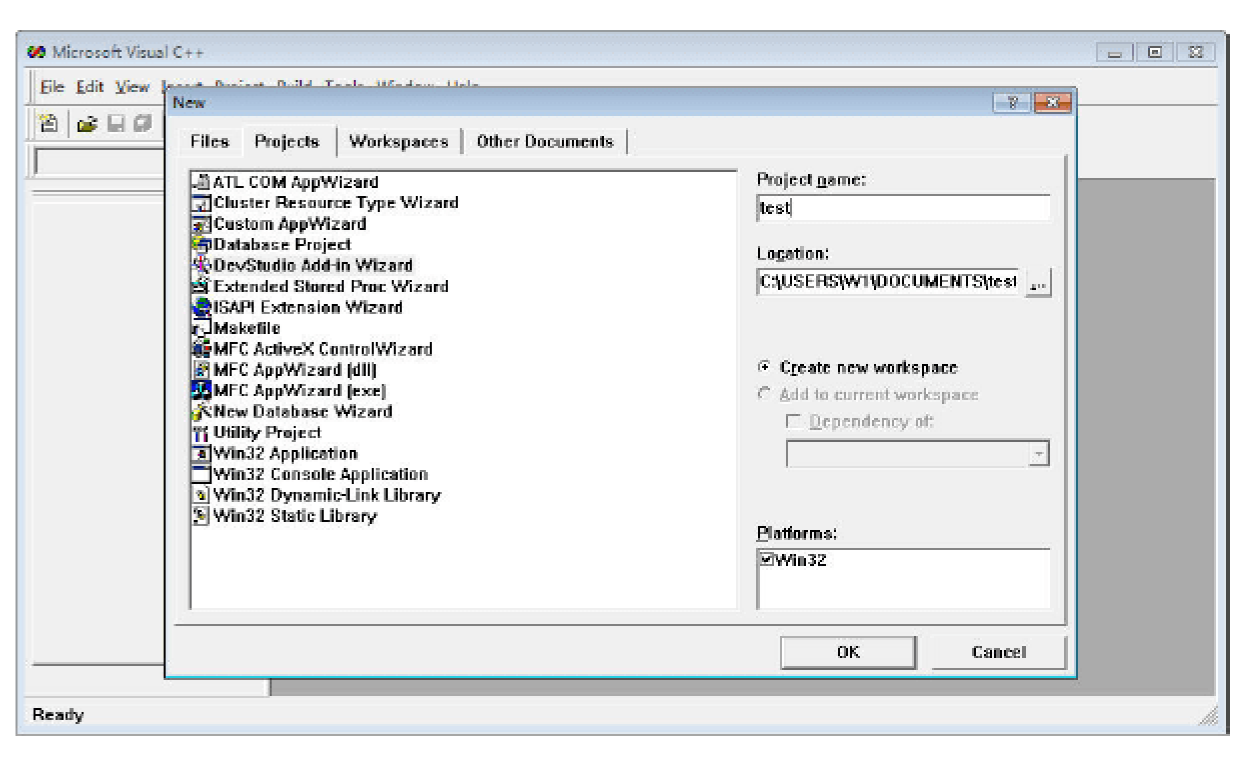




图 13-31 运行发布的程序

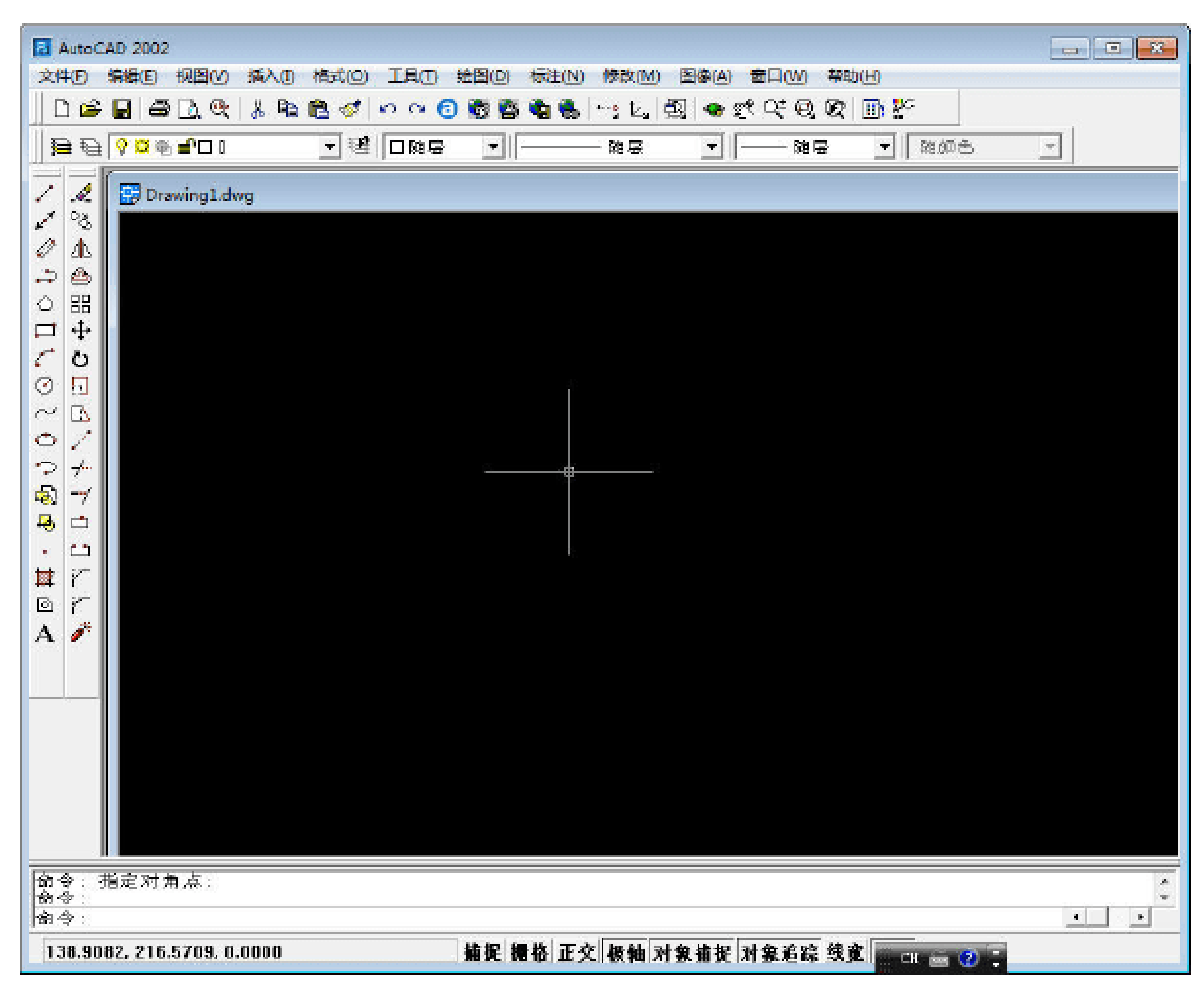


图 13-32 AutoCAD 运行界面

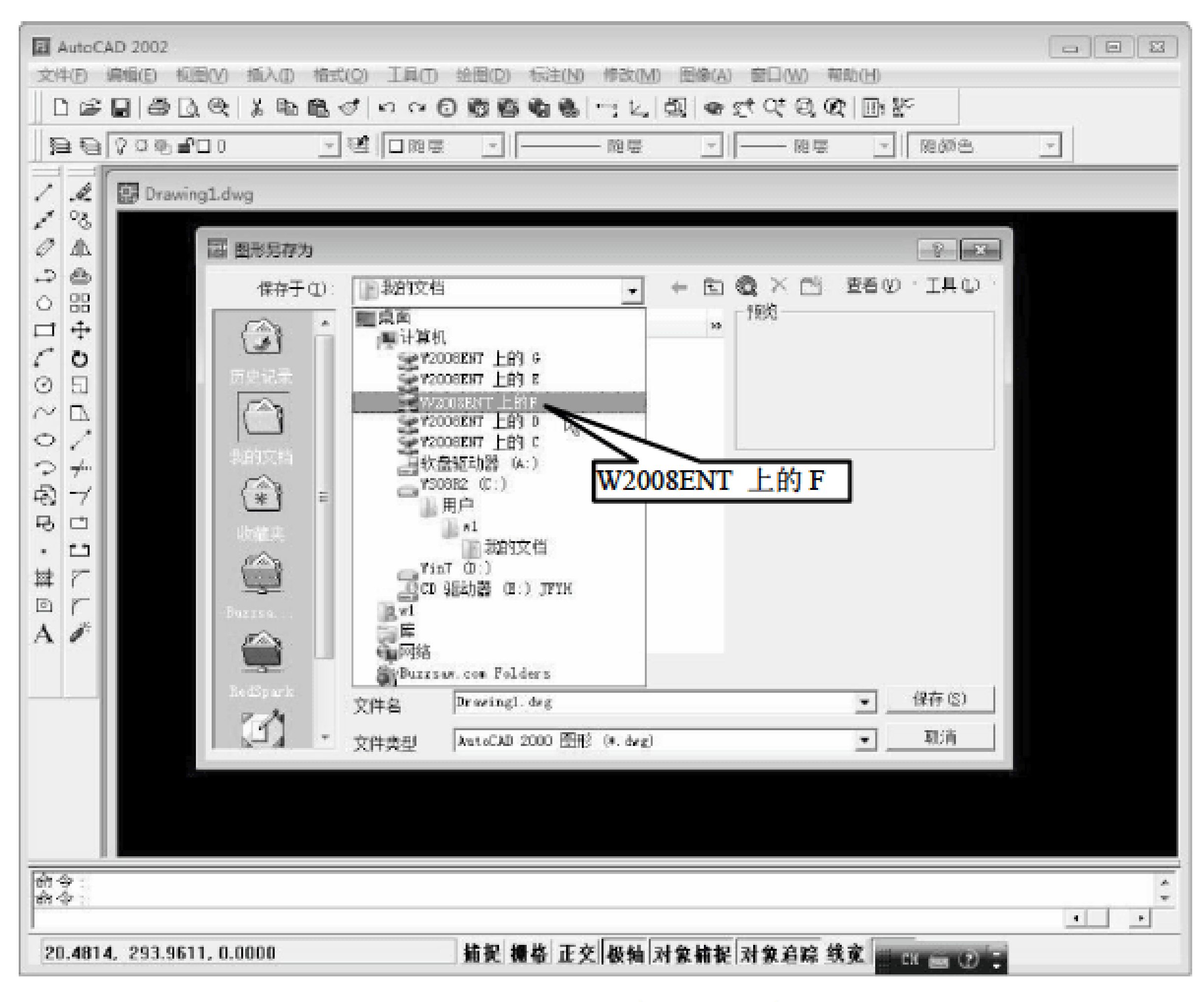


图 13-33 本地磁盘

13.4.2　通过 RDP 文件访问服务器提供的 RemoteApp 程序

除了以 Web 方式连接并运行服务器端的 RemoteApp 程序外，还可以通过“网络共享”的方式，直接运行服务器端发布的 RDP 文件，主要操作步骤如下。

01 在工作站端，以“文件共享”的方式，访问服务器发布的 RDP 共享文件夹，如图 13-34 所示。

02 用鼠标双击其中的一个 RDP 文件，进入远程桌面连接对话框，输入服务器提供的用户名、密码，然后单击“确定”按钮，如图 13-35 所示。

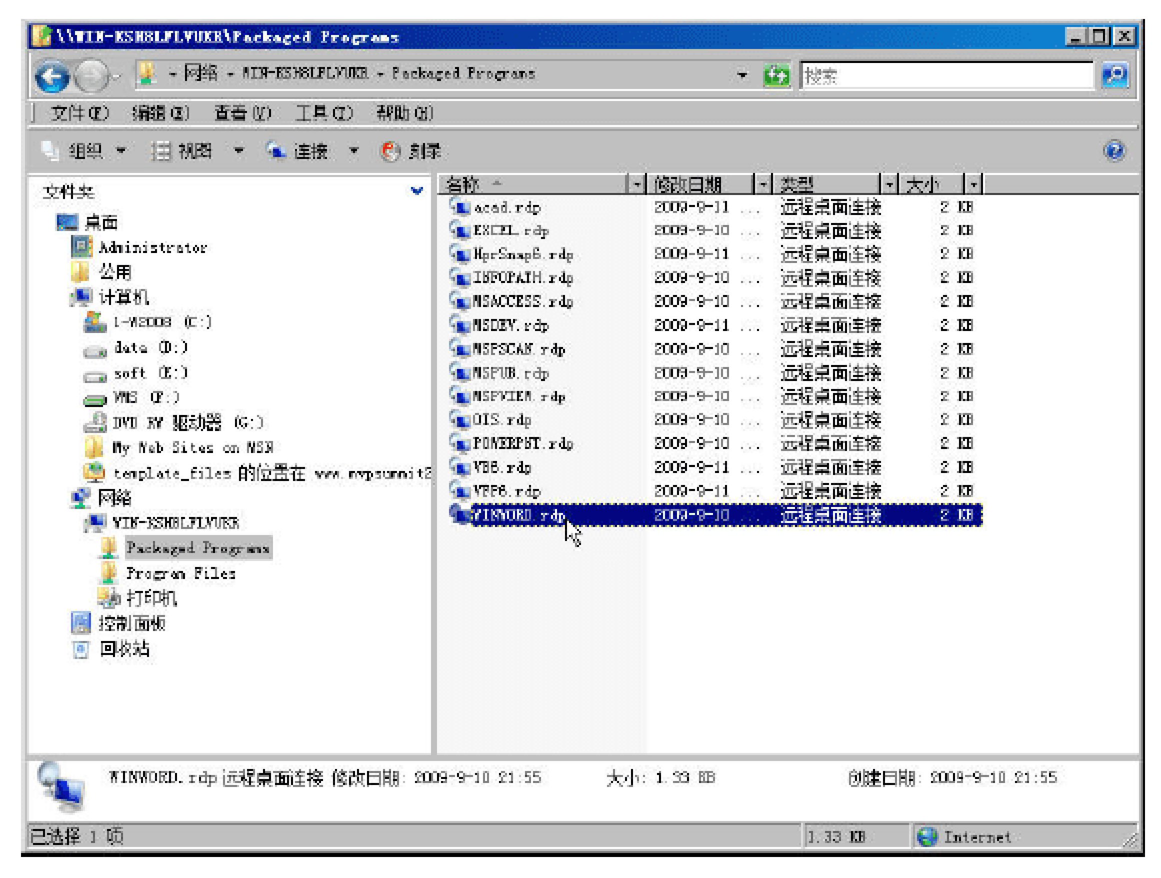



图 13-34　连接到服务器提供的共享文件夹

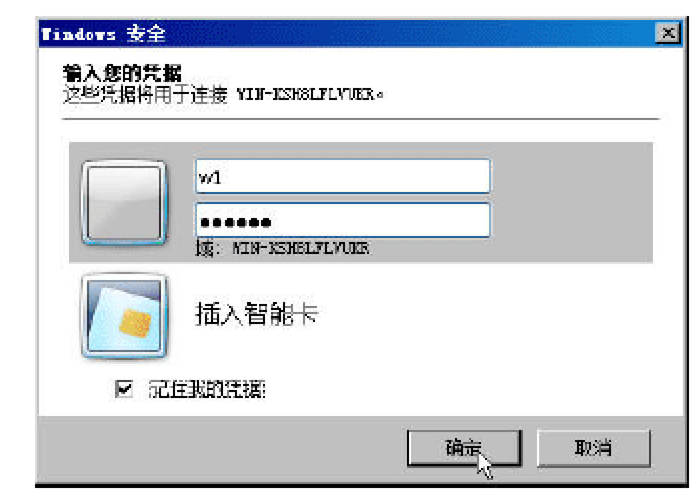


图 13-35　连接到服务器

03 之后就可以运行服务器端发布的程序了，如图 13-36 所示。

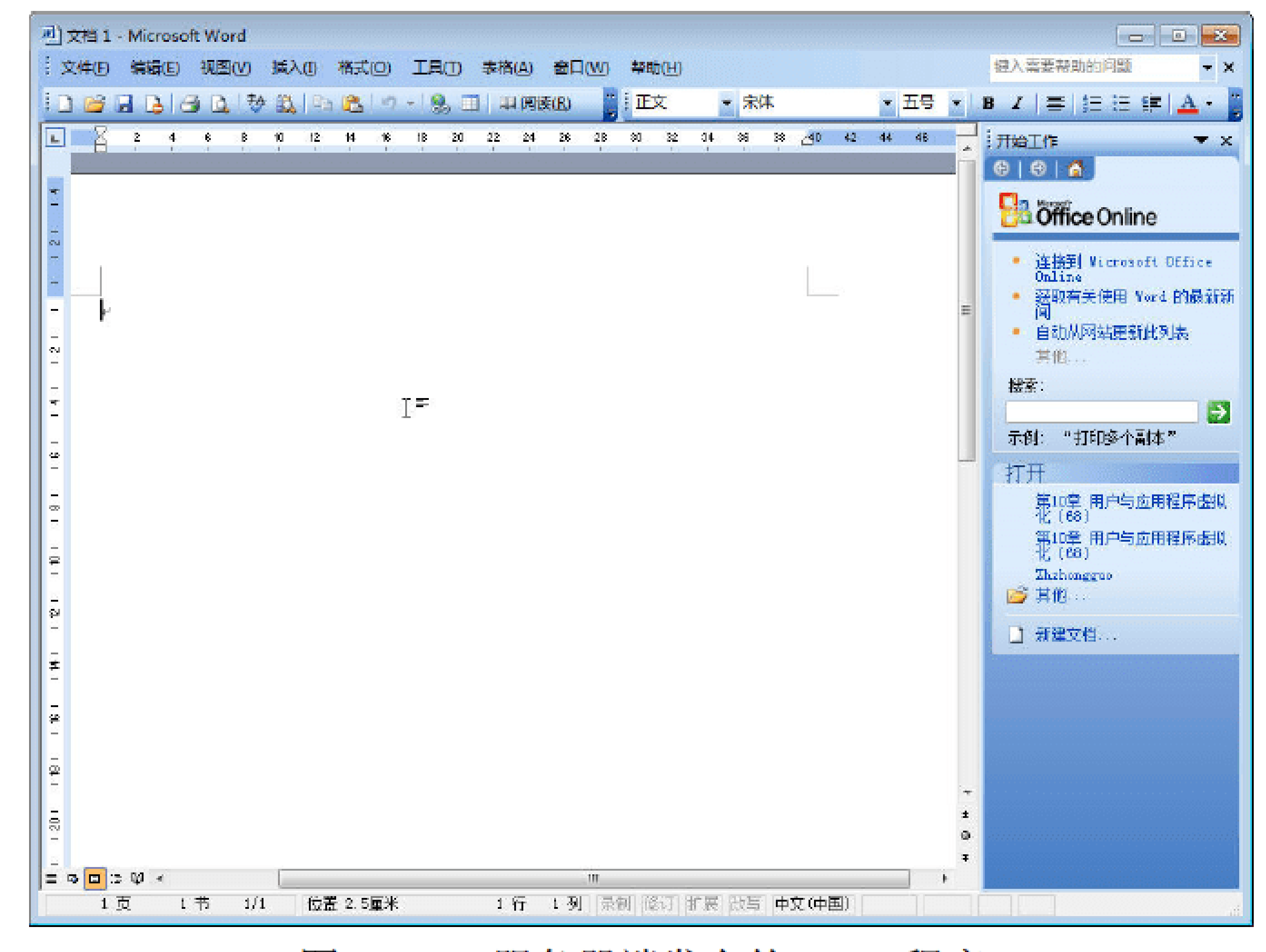


图 13-36　服务器端发布的 Word 程序

13.4.3　通过 Windows Installer 程序包访问服务器发布的 RemoteApp 程序

除了上述 2 种方式以外，还可以通过 Windows Indtaller 程序包访问服务器发布的 RemoteApp

程序，主要步骤如下。

01 在打开图 13-34 所示的共享后，还可以看到服务器端发布的“Windows Installer”程序包，如图 13-37 所示，双击某个程序包。

02 在弹出的“打开文件-安全警告”对话框中，单击“运行”按钮，如图 13-38 所示。

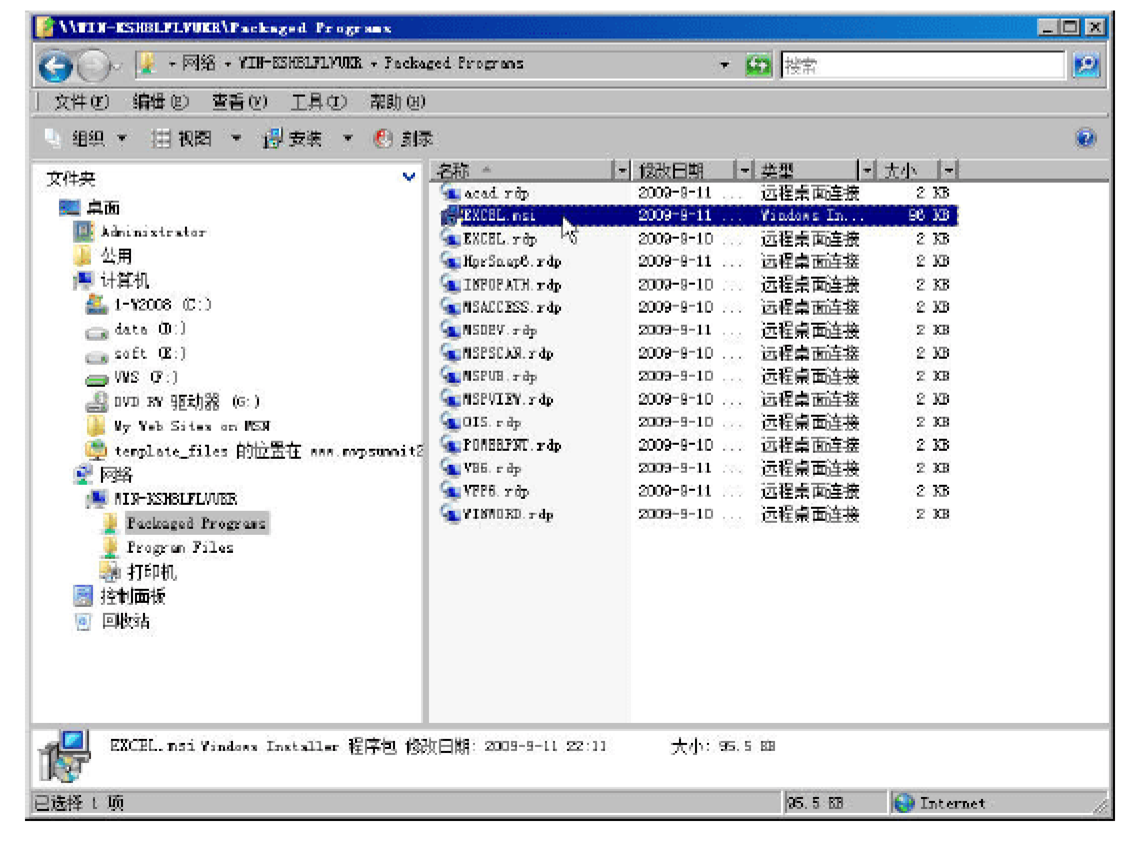


图 13-37　安装 MSI 程序

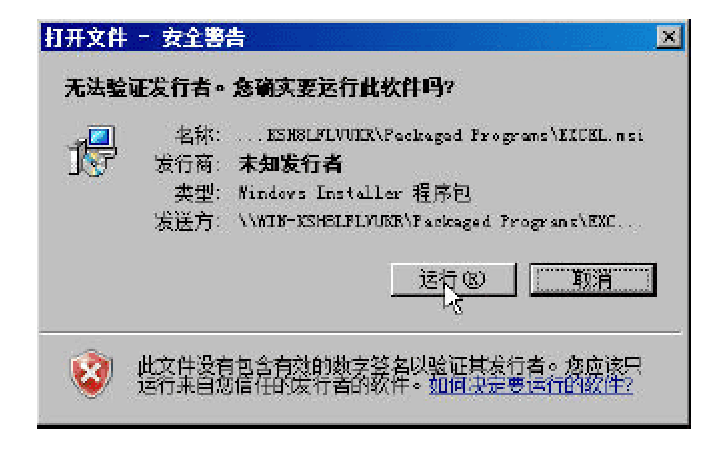


图 13-38　运行程序

03 Windows Installer 程序将开始安装，这个过程很快，只有几秒种的时间，如图 13-39 所示。

04 程序安装完成后，可以在“开始菜单→程序→远程程序”程序组中看到新安装的程序，如图 13-40 所示。



图 13-39　安装程序到工作站

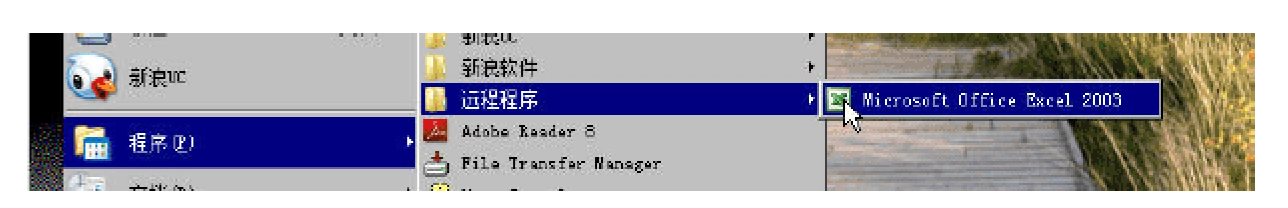
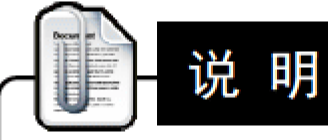


图 13-40　安装到工作站端的程序

05 运行这个程序，会进入“远程桌面”启动页，如图 13-41 所示。



说 明

在图 13-41 的远程桌面连接时，不需要输入用户名和密码。

06 随后就会进入运行的程序，这是一个 Excel 的程序，如图 13-42 所示。



图 13-41　远程桌面连接



图 13-42　运行的程序

通过网络改造后， RemoteApp 总体效果良好。在实际使用中，发现直接双击 rdp 使用发布的 RemoteApp 程序，要比使用网站中运行的速度快些。而通过 Web 方式，则不需要再打开“文件夹共享”，也不像安装 Windows Installer 包一样，必须安装的软件才能使用，而是可以通过浏览服务器端发布的软件，来选择所需要的软件。所以，在实际使用中，如果网络中有“域控制器”，而工作站都加入到了“域”，选择在“组策略”中使用软件发布“Windows Installer 程序包”的方式，则是最简单、方便的；如果网络中没有“域控制器”，则采用“Web 站点”方式比较合适。

第 4 篇

高级与综合网络应用



第 14 章　从 Windows Server 2003 升级到 Windows Server 2008 R2

如果网络中已经存在 Windows Server 2003，并且是 Active Directory 的网络，想将网络升级到 Windows Server 2008 或 Windows Server 2008 R2，则需要遵循一定的步骤才可以完成升级。为了让大家掌握这一内容，本章将通过两个案例，介绍升级的步骤。

14.1　升级到 Windows Server 2008 R2 的原则

如果要将 Windows Server 2003 升级到 Windows Server 2008 或 Windows Server 2008 R2，有两种升级方法，一种是“直接”升级，即直接将 Windows Server 2003 升级到 Windows Server 2008 或 Windows Server 2008 R2；另一种是当不能直接升级到 Windows Server 2008 或 Windows Server 2008 R2 的时候，可以通过“间接”升级的方式完成升级。

在“直接”升级的时候，需要遵循如下原则：

（1）只能从同一版本升级到更高版本，不能跨版本升级。例如，你可以将 Windows Server 2003 标准版升级到 Windows Server 2008 的标准版，但不能将 Windows Server 2003 的标准版升级到 Windows Server 2008 的企业版。

（2）不能跨平台升级。例如，可以从 32 位的 Windows Server 2003 升级到 32 位的 Windows Server 2008，或者从 64 位的 Windows Server 2003 升级到 64 位的 Windows Server 2008 或 Windows Server 2008 R2，但不能从 32 位的 Windows Server 2003 升级到 64 位的 Windows Server 2008。

（3）不能跨语言版本。例如，只能从英文版的 Windows Server 2003 升级到英文版的 Windows Server 2008，但不能升级到中文版的 Windows Server 2008 等。

（4）除了满足上述要求外，还要符合升级到 Windows Server 2008 及 Windows Server 2008 R2 的最低软、硬件要求（主要是 CPU 与磁盘空间，尤其是系统盘空间需求）。例如，如果要升级到 Windows Server 2008 的 64 位版本，则服务器的硬件需要是 64 位的 CPU。

凡是不能满足上述直接升级要求的任意一条，都只能通过“间接”升级的方式，将网络中的 Windows Server 2003 升级到 Windows Server 2008。例如，用户当前安装的是 Windows Server 2003 的标准版（32 位），想将其升级到 Windows Server 2008 R2（只有 64 位产品），则可以通过如下的方式进行升级：

（1）如果原来的服务器 A，不能满足 64 位的 Windows Server 2008 R2 的需求，则只能通过新购买服务器 B 的方式，将新购买的服务器 B 连接到网络，安装 Windows Server 2008 R2，并升级到“主域”控制器，原服务器 A 降级到“额外”域控制器，然后从 Active Directory 中脱离。新的服务器 B 代替原来的服务器 A 工作，这是一种升级方式。最后，将 B 的 IP 地址、子网掩码、网关、DNS 设置成 A 的相关参数。

（2）如果原来的服务器 A，能满足 64 位的 Windows Server 2008 R2 的需求，则可以通过一台“中间”的服务器 B，将 B 接入网络，安装 Windows Server 2008 R2，并升级到“主域”控制器，然后服务器 A 降级成“额外”域控制器，从 Active Directory 中脱离；然后备份 A 中的数据到其他服务器后，将 A 重新分区、格式化，安装 Windows Server 2008 R2，并升级到“主域”控制器，中间服务器 B 降级成“额外”域控制器，从域中脱离；这样可以完成整个升级的过程。

14.2　直接从 Windows Server 2003 升级到 Windows Server 2008

在本节中，通过一个具体的实例，介绍从 Windows Server 2003 企业版“直接”升级到 Windows Server 2008 企业版的内容，步骤如下。

01 现有一个 Windows Server 2003 的 Active Directory 服务器，域名为 dc.heinfo.local，如图 14-1 所示。

02 当前的产品是 Windows Server 2003 的 32 位的企业版，如图 14-2 所示。

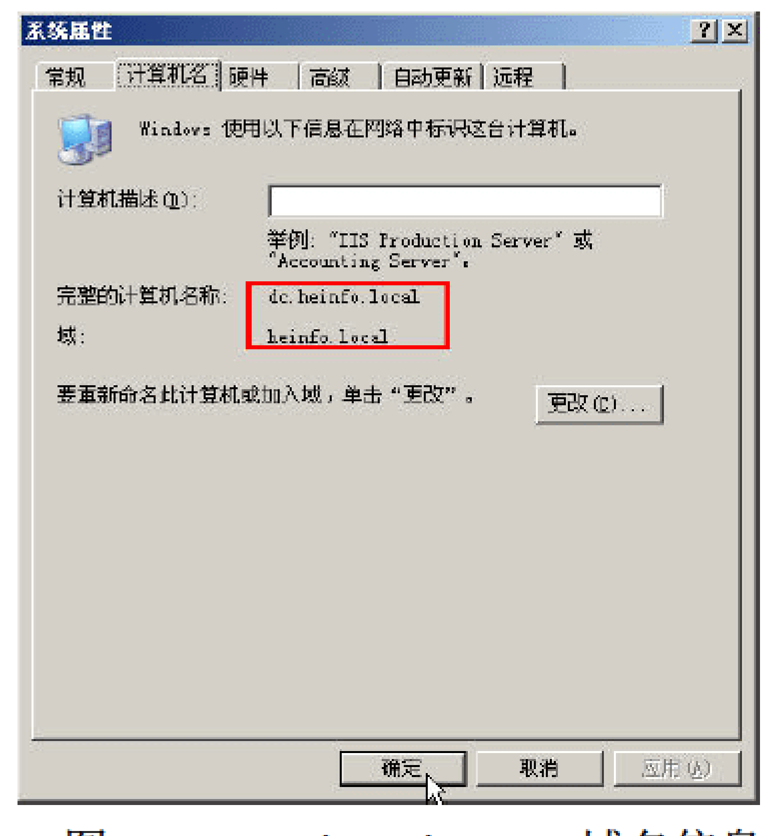


图 14-1　Active Directory 域名信息

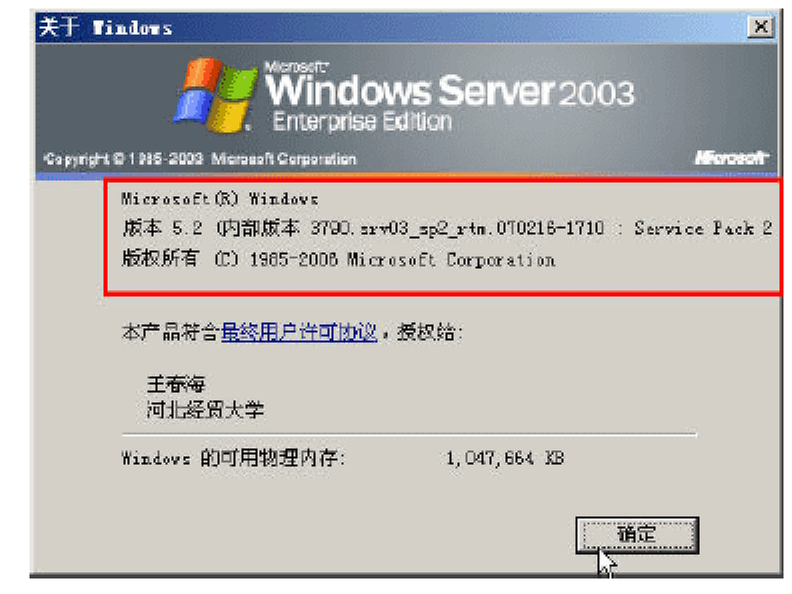


图 14-2　Windows Server 2003 企业版

03 打开“Active Directory 用户和计算机”窗口，右击域名，在弹出的快捷菜单中选择“提升域功能级别”命令，如图 14-3 所示。

04 在弹出的“提升域功能级别”对话框中，在“选择一个可用的域功能级别”下拉列表中选择“Windows Server 2003”选项，如图 14-4 所示。然后单击“提升”按钮，完成域功能级别的提升。

05 更新林信息。

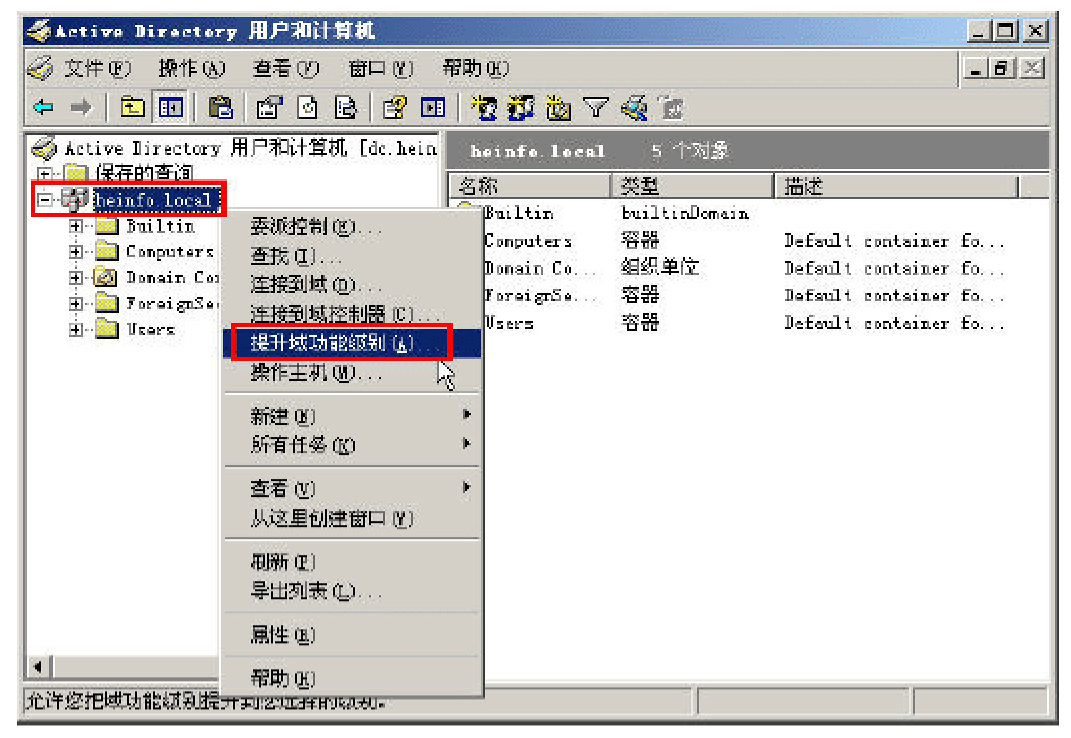


图 14-3　Active Directory 用户和计算机

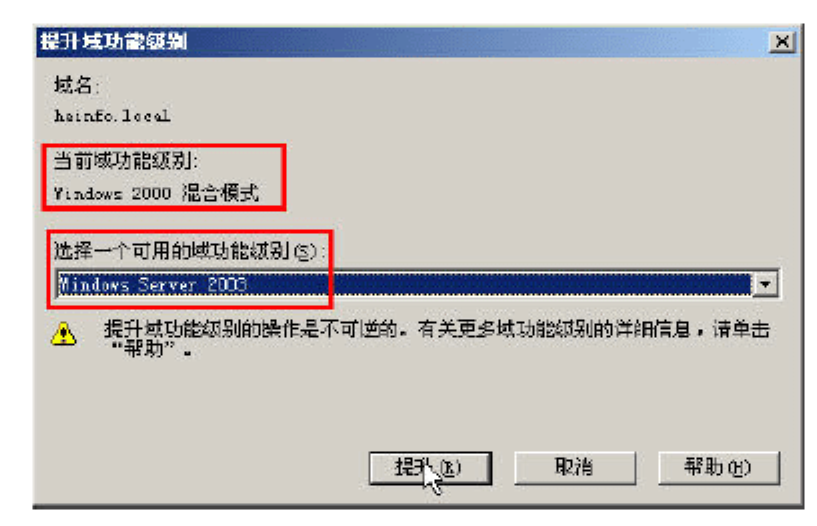


图 14-4　提升域功能级别

将 Windows Server 2008 的 32 位的安装光盘，插入服务器光驱中，或者使用光盘镜像文件，利用虚拟光驱软件加载。在本例中，Windows Server 2008 安装光盘所在盘符为 D 盘。进入命令提示符，执行如下命令：

```
d:
cd  \support\adprep
adprep  /forestprep
```

如图 14-5 所示，在提示输入 C 继续时输入 C，然后按回车键。Windows Server 2008 的 Active Directory 准备工具将升级 Windows Server 2003 的林到 Windows Server 2008 的林。

06 然后执行 adprep /domainprep，更新域控制器信息，如图 14-6 所示。

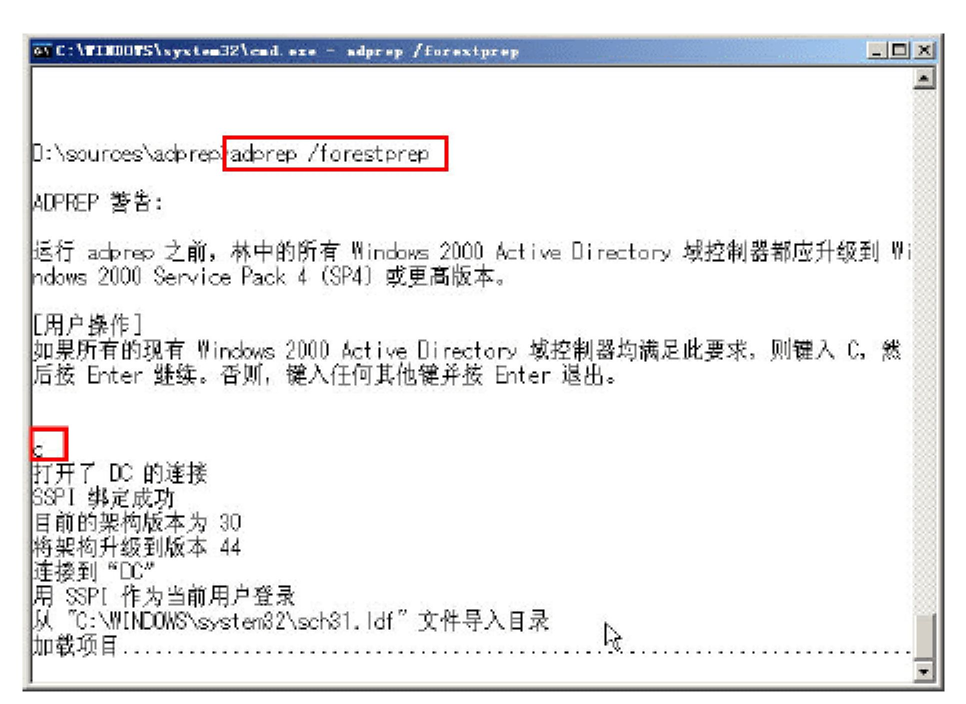


图 14-5　更新林信息

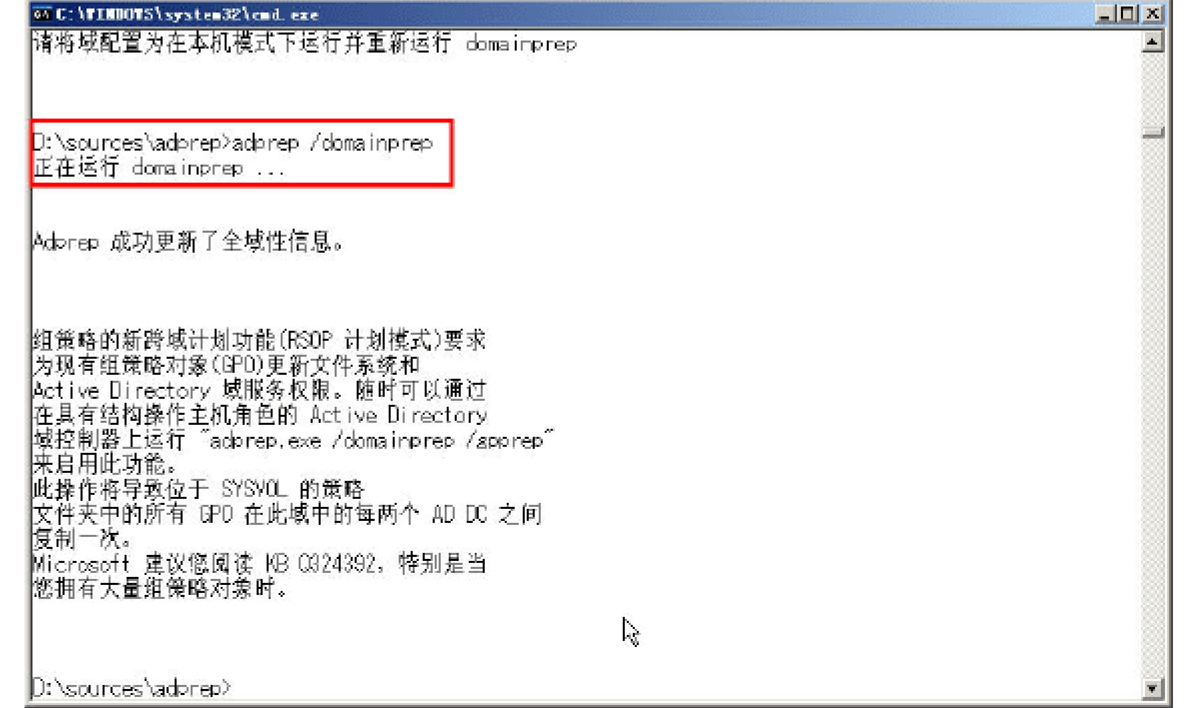


图 14-6　更新域控制器信息

07 最后执行 adprep /domainprep /gpprep 更新全域信息，如图 14-7 所示。

08 更新林信息、域信息完成之后，运行 Windows Server 2008 的安装程序，在"选择要安装的操作系统"对话框中，选择与要升级的 Windows Server 2003 相同的产品，如图 14-8 所示。本例中为 Windows Server 2008 Enterprise（完全安装）。

09 在"您想进行何种类型的安装"中，选择"升级"，如图 14-9 所示。

10 在"兼容性报告对话框中，单击"下一步"按钮，如图 14-10 所示。

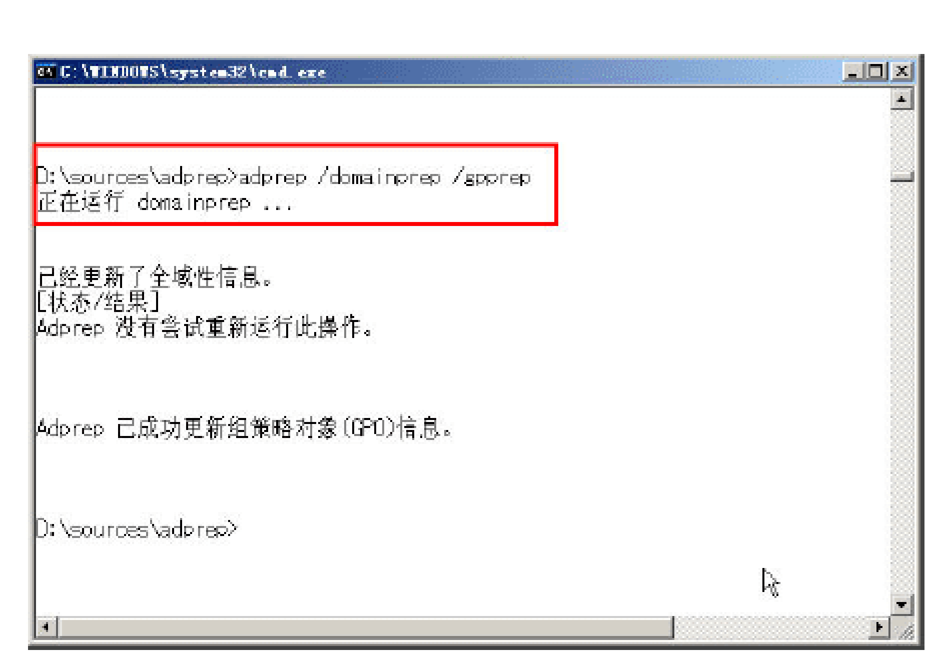


图 14-7　更新全域信息

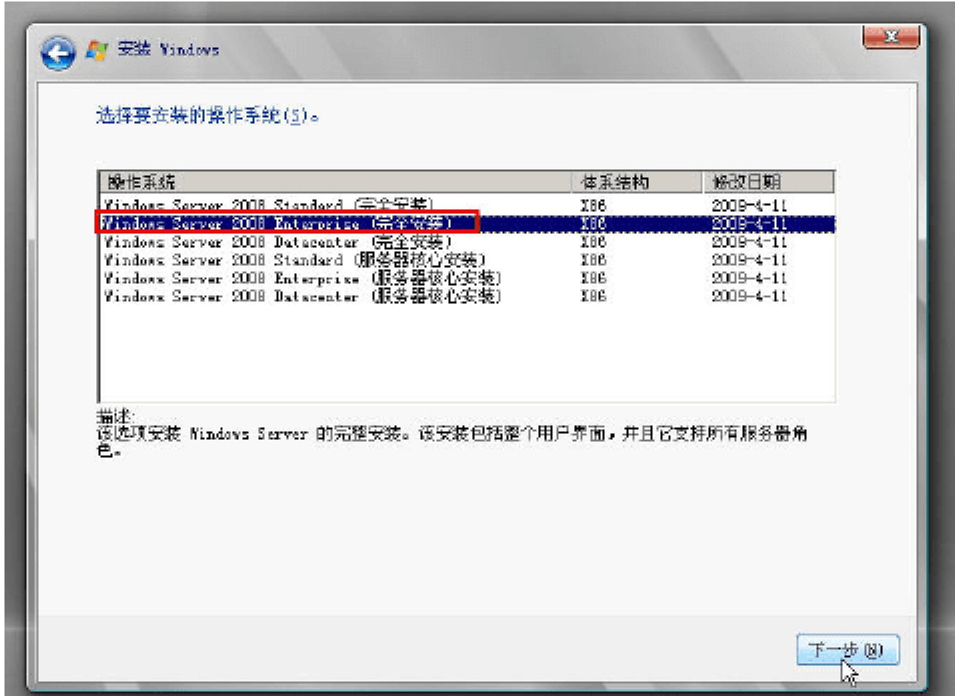


图 14-8　选择操作系统

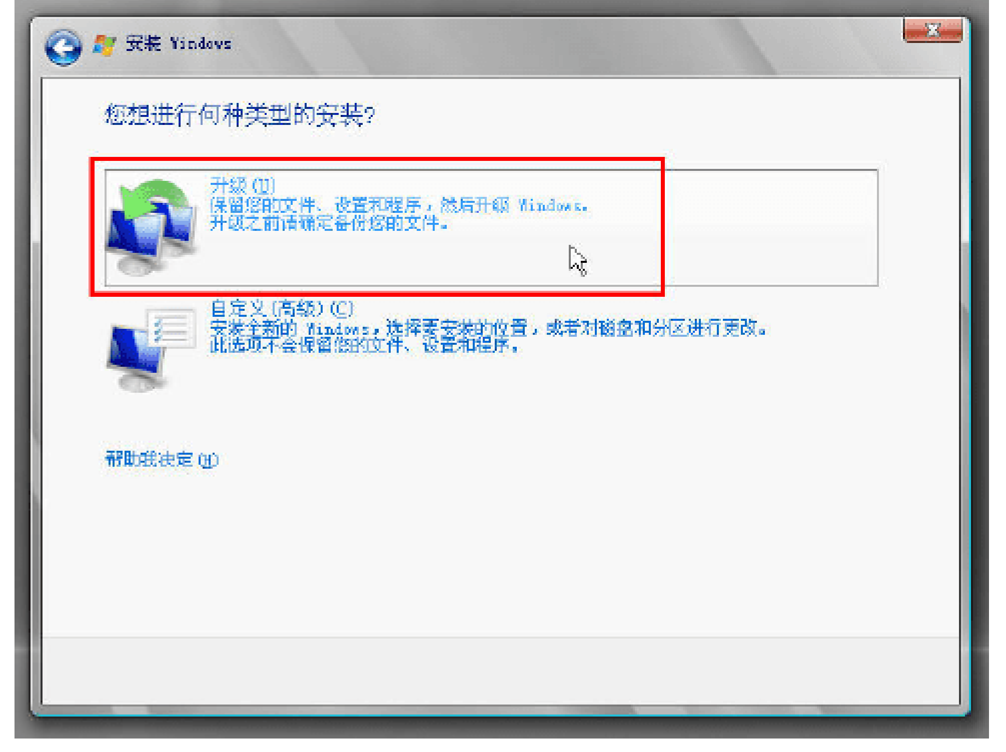


图 14-9　升级

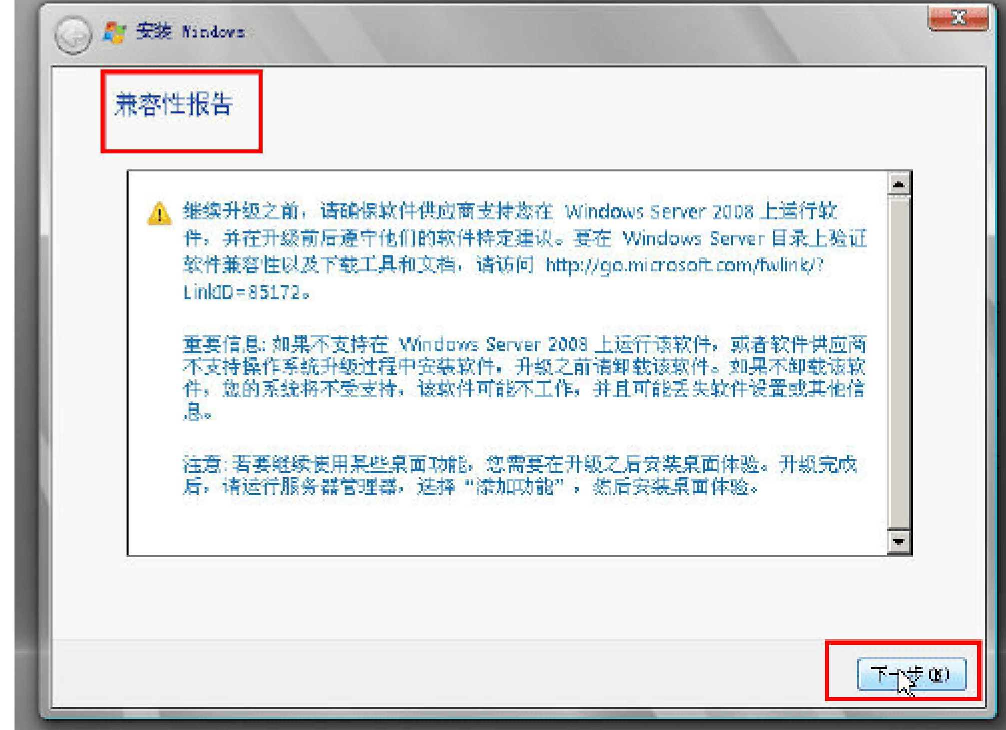


图 14-10　兼容性报告

11 随后，Windows Server 2008 的安装程序将开始进行升级安装，如图 14-11 所示。

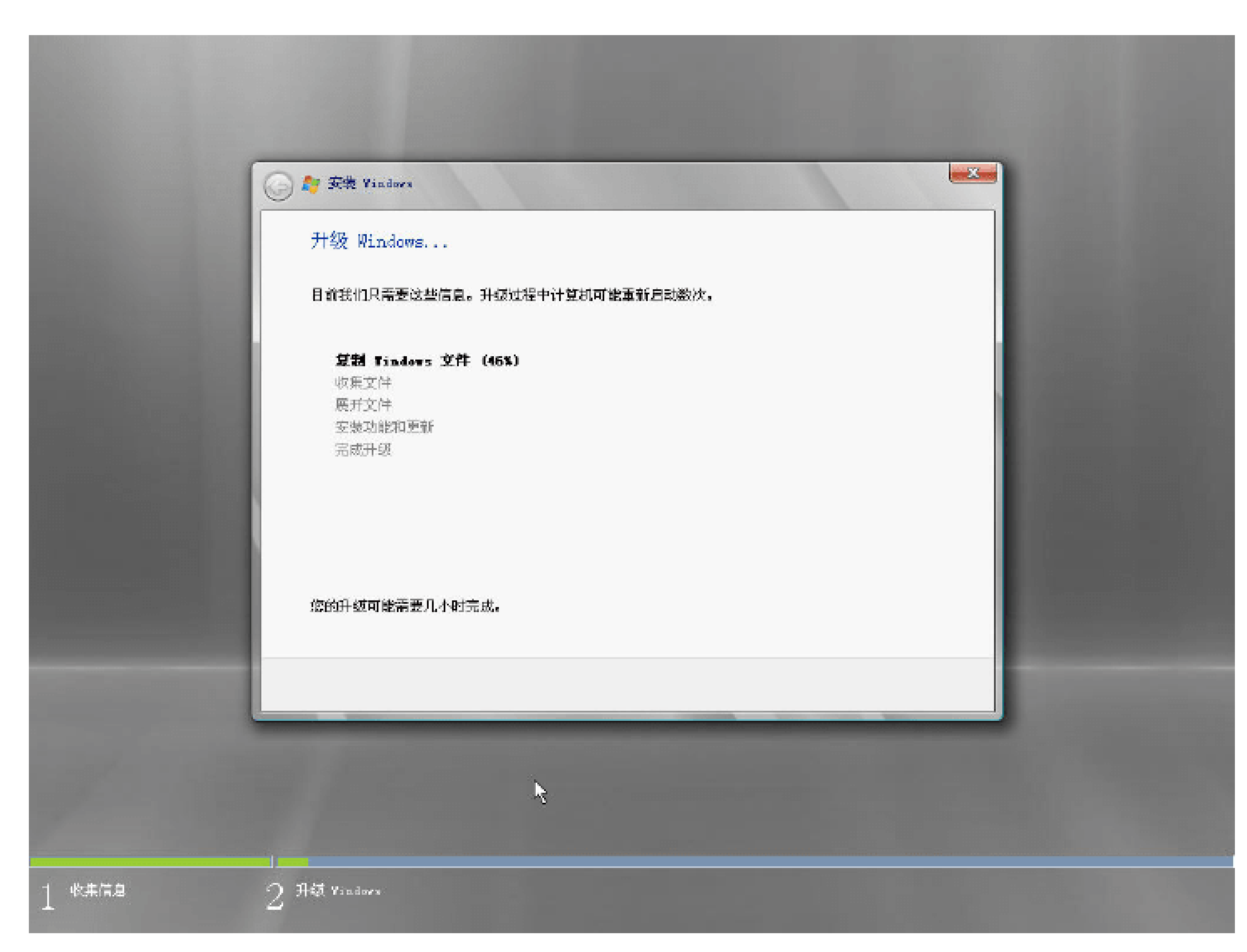


图 14-11　升级 Windows

12 最后会完成 Windows Server 2008 的升级，如图 14-12 所示。

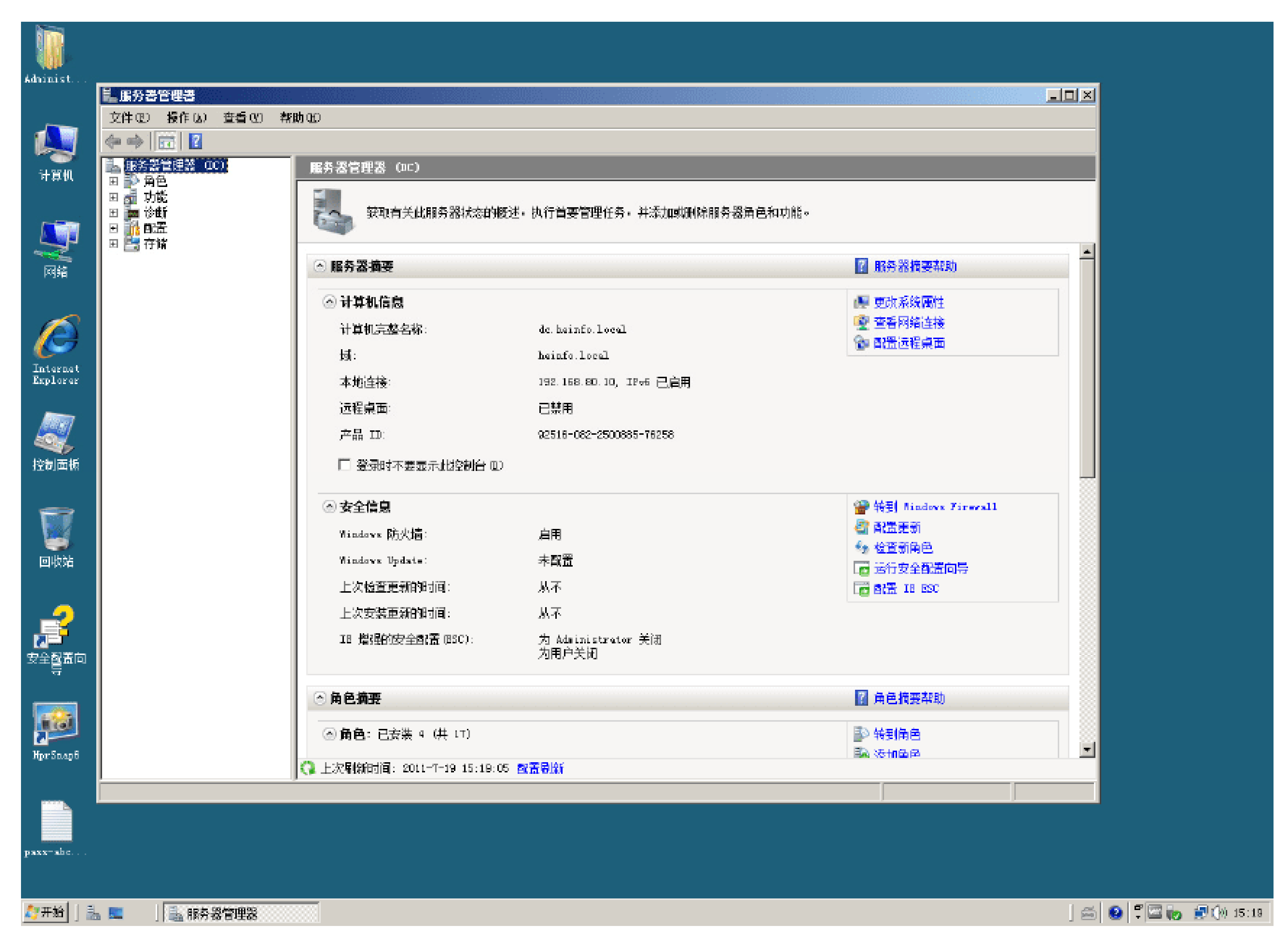


图 14-12 完成 Windows Server 2008 的升级

14.3 通过中间服务器升级到 Windows Server 2008 R2

如果 Windows Server 2003 服务器（假设为 A 服务器），不满足升级到新版 Windows Server 2008 或 Windows Server 2008 R2 的要求，则可以通过“中间”服务器（假设为 B 服务器），完成升级。下面通过具体的实例，介绍这个内容。

14.3.1 在 Windows Server 2003 升级域信息

当前网络中有一台 Windows Server 2003 服务器（A，计算机名称为 dc.heinfo.local），想要将其升级到 Windows Server 2008 R2，由于 Windows Server 2003 是 32 位的版本，而 Windows Server 2008 R2 是 64 位，所以不能直接升级。并且其 C 盘空间只有 6GB，所以，想通过“中间服务器”的方式完成升级，主要步骤如下。

01 这台即将升级的 Windows Server 2003 的 IP 地址是 192.168.80.10，DNS 是 192.168.80.10，如图 14-13 所示。

02 打开“Active Directory 用户和计算机”窗口，右击域名，在弹出的快捷菜单中选择“提升域功能级别”命令，在弹出的“提升域功能级别”对话框中，选择“Windows Server 2003”，如图 14-14 所示。然后单击“提升”按钮，完成域功能级别的提示。

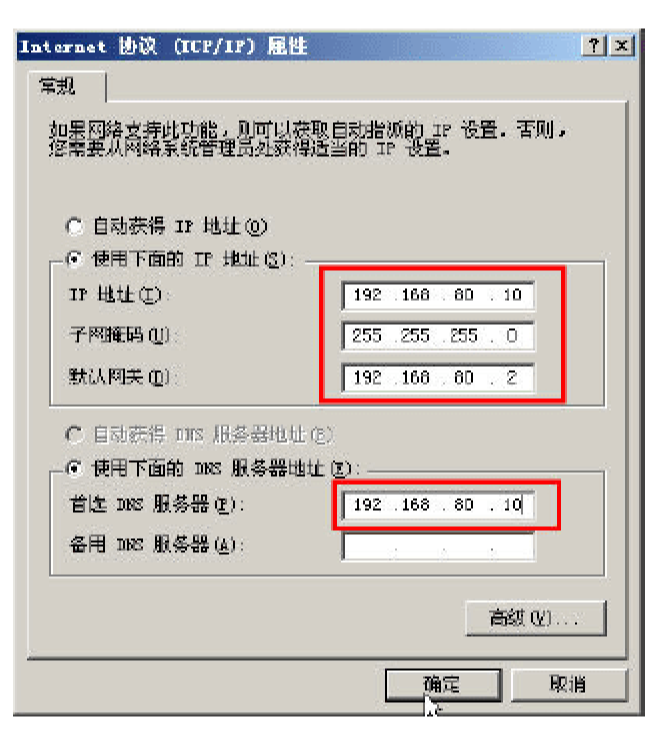


图 14-13　服务器 IP 地址与 DNS

图 14-14　提升域功能级别

03 更新林信息。

将 Windows Server 2008 R2 的安装光盘，插入服务器光驱中，或者使用光盘镜像文件，利用虚拟光驱软件加载。在本例中，Windows Server 2008 R2 安装光盘所在盘符为 E 盘。进入命令提示符，执行如下命令：

```
e:
cd   \support\adprep
adprep32   /forestprep
```

如图 14-15 所示，在提示输入 C 继续时，输入 C，然后按回车键。Windows Server 2008 的 Active Directory 准备工具将升级 Windows Server 2003 的林到 Windows Server 2008 的林。



说 明

如果要升级 64 位的 Windows Server 2003 的 Active Directory 信息，可以执行 adprep.exe，这是 64 位的升级程序。

04 然后执行 adprep32 /domainprep，更新域控制器信息，如图 14-16 所示。

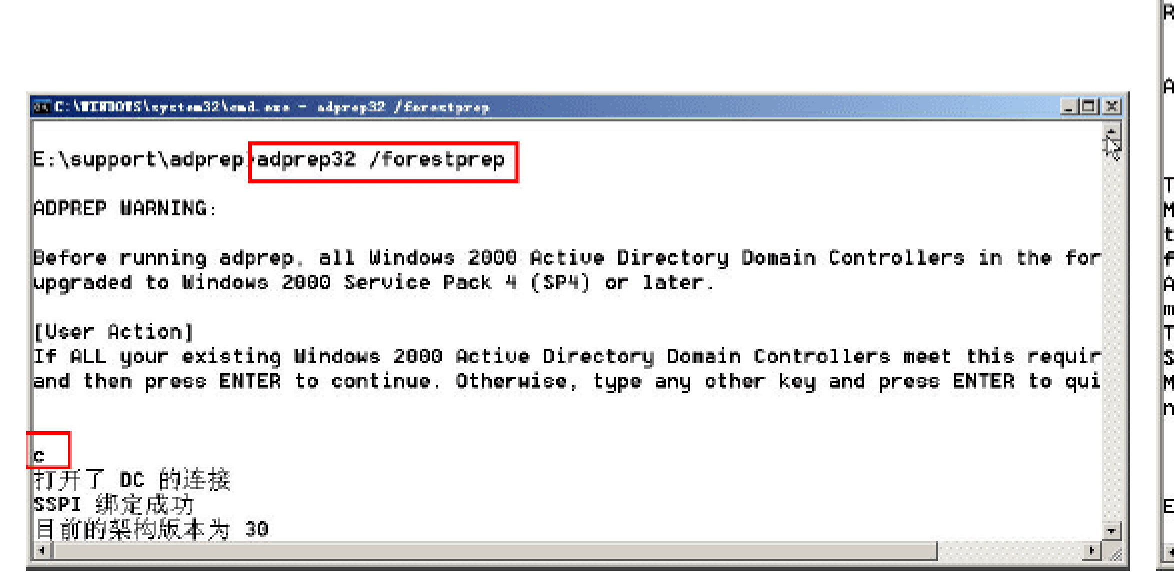


图 14-15　更新林信息

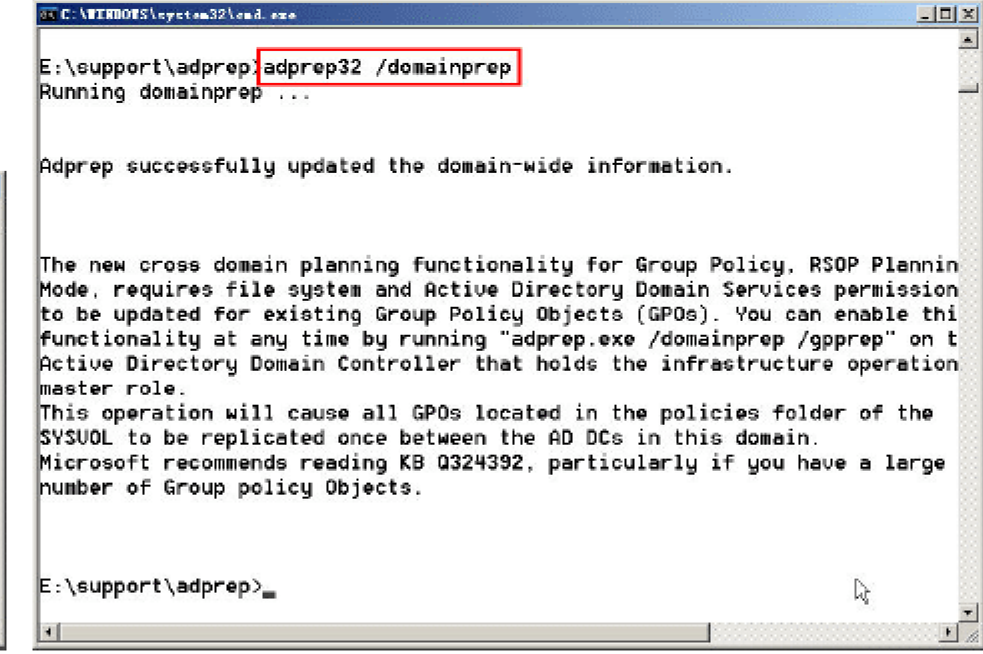


图 14-16　更新域控制器信息

05 最后执行 adprep32 /domainprep /gpprep 更新全域信息，如图 14-17 所示。

06 如果以后要在网络中安装只读域控制器，需要执行 adprep32 /rodprep，如图 14-18 所示。

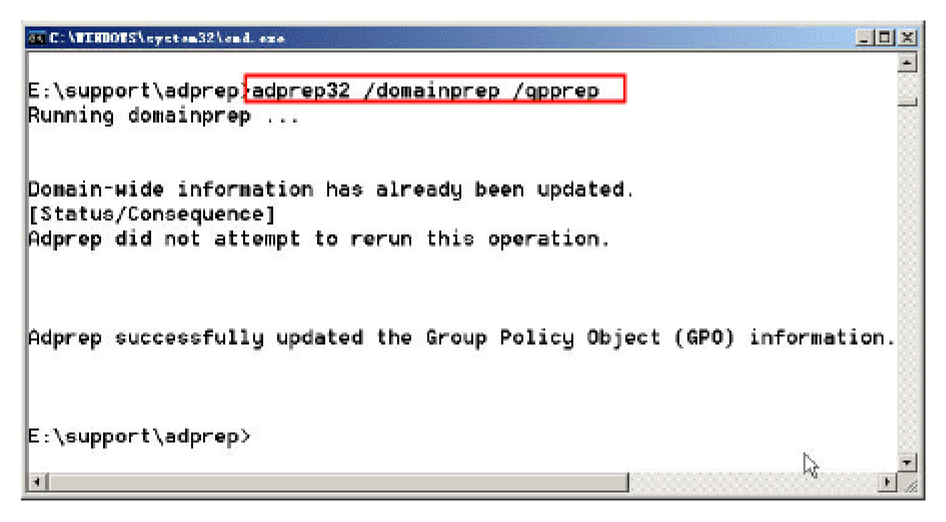



图 14-17　更新全域信息

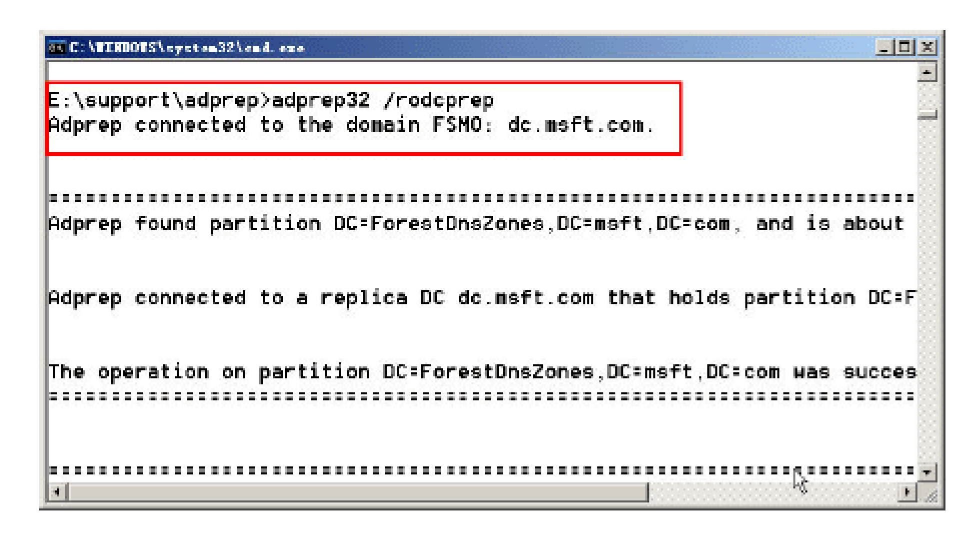


图 14-18　为安装只读域控制器更新信息

14.3.2　将中间服务器 B 升级到额外域控制器

在“中间服务器”上安装 Windows Server 2008 R2，修改计算机名称，设置 IP 地址，将其加入到现有的域中，主要步骤如下。

01 在服务器 B 上，安装 Windows Server 2008 R2，并修改计算机名称为 AD，如图 14-19 所示。


说 明

修改计算机名称之后，根据提示，重新启动计算机。

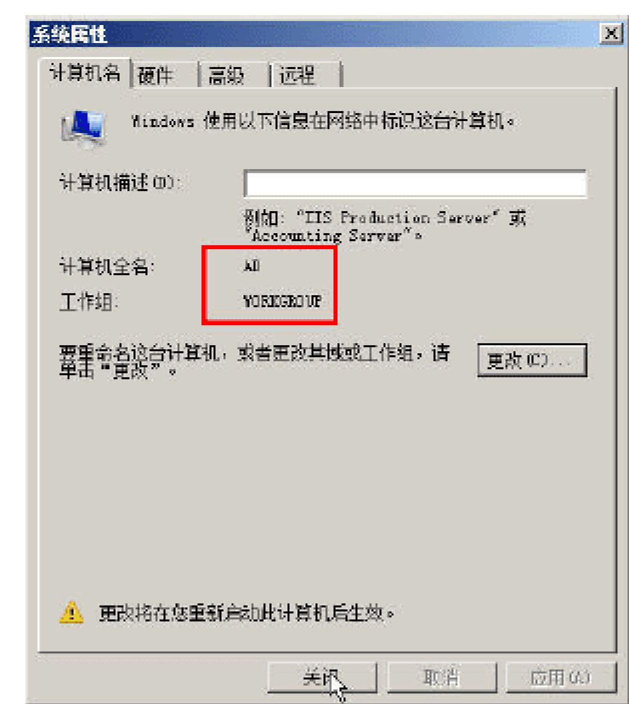


图 14-19　修改计算机名称

02 进入系统后，设置 IP 地址为 192.168.80.11，DNS 地址为服务器 A 的地址 192.168.80.10，如图 14-20 所示。

03 然后运行 dcpromo，进入“Active Directory 域服务安装向导”，在“选择某一部署配置”对话框中，选中“现有林→向现有域添加域控制器”单选按钮，如图 14-21 所示。

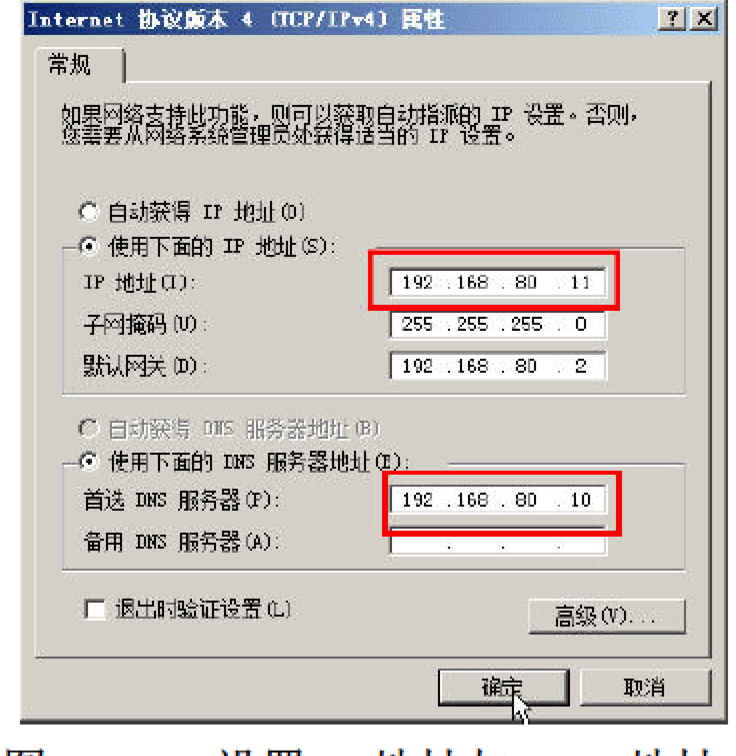


图 14-20　设置 IP 地址与 DNS 地址

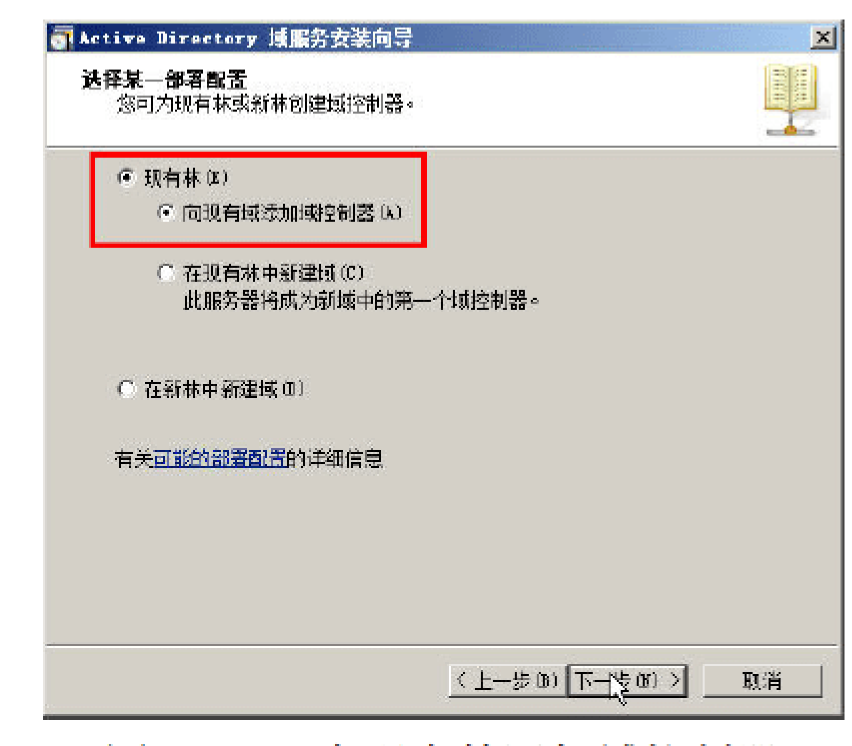


图 14-21　向现有林添加域控制器

04 在“网络凭据”对话框中，在“输入位于计划安装此域控制器的林中任何域的名称”文本框中，输入当前网络中的域名，本例为 msft.com，然后单击“设置”按钮，在“网络凭据”对话框中，输入域管理员账户与密码，如图 14-22 所示。



图 14-22　网络凭据

05 在“选择域”对话框中，选择现有的域，如图 14-23 所示。

06 在“请选择一个站点”对话框中，为新域控制器选择一个站点，如图 14-24 所示。



图 14-23　选择域

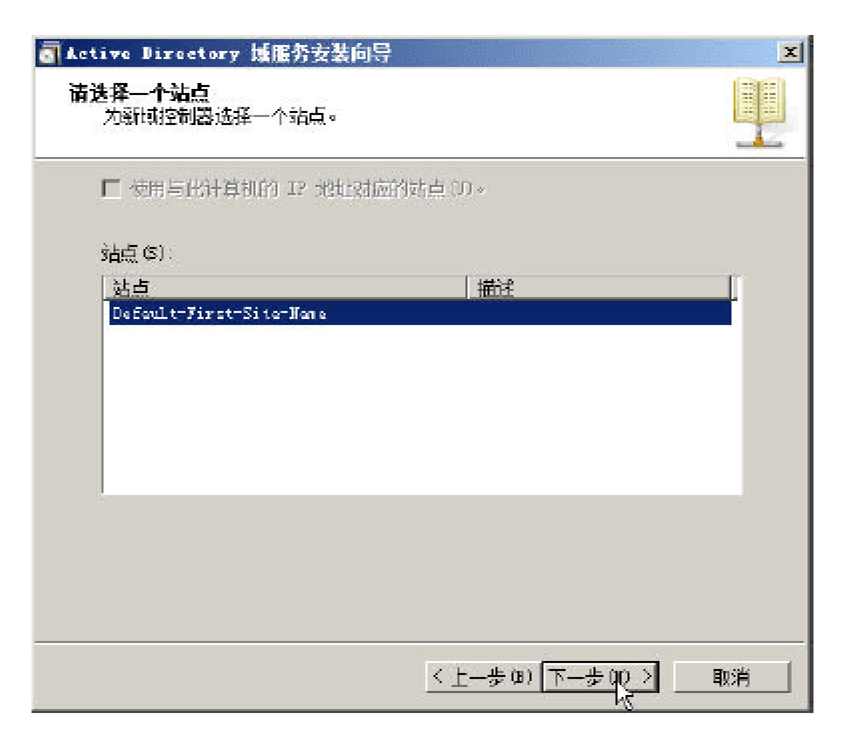


图 14-24　为新域控制器选择一个站点

07 在“其他域控制器选项”对话框中，选中默认值“DNS 服务器”与“全局编录”复选框，如图 14-25 所示。

08 “Active Directory 域服务安装向导”的其他步骤，则与升级到 Active Directory 相似，这里不一一介绍。在“等待 DNS 安装完成”对话框中，选中“完成后重新启动”复选框，如图 14-26 所示。在加入到 Active Directory 并成为额外域控制器之后，系统会自动重启。

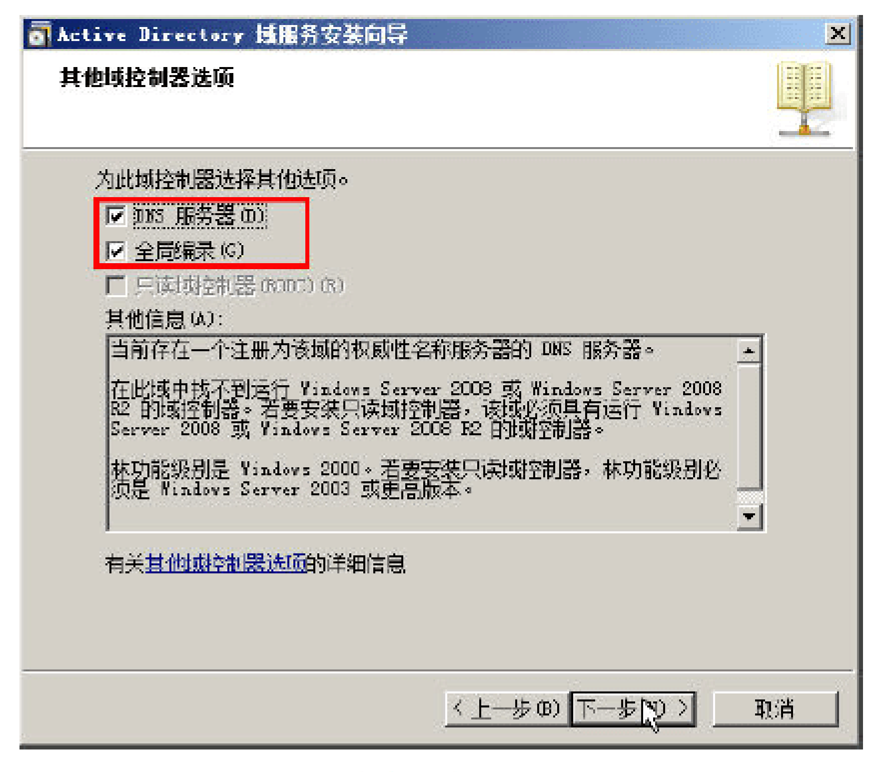


图 14-25　其他域控制器选项

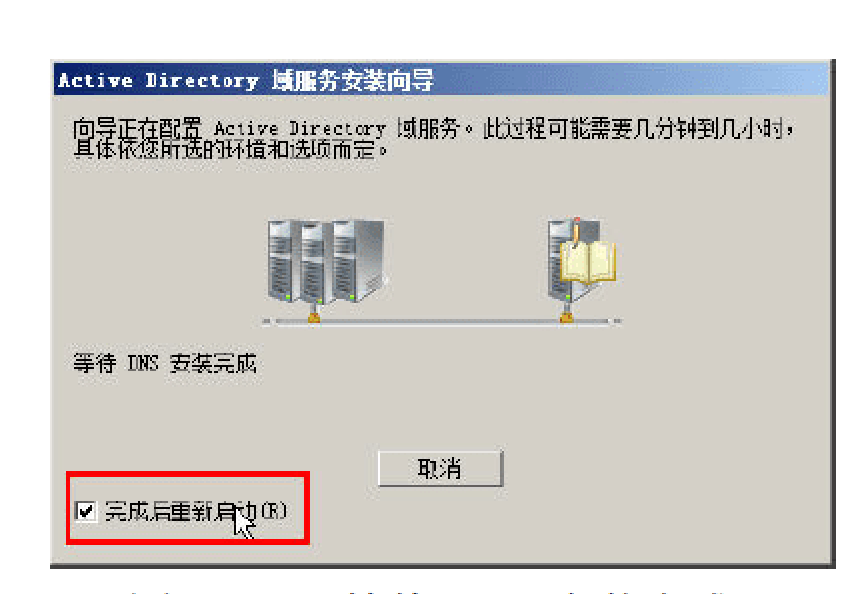


图 14-26　等待 DNS 安装完成

14.3.3　将中间服务器 B 升级到主域控制器

在将中间服务器 B 加入到 Active Directory 并成为“额外域控制器”之后，接下来要将这台服务器升级到“主域控制器”，主要步骤如下。

01 在服务器 B 中，打开“服务器管理器”窗口，定位到“角色→Active Directory 域服务→Active Directory 用户和计算机”，右击域名，在弹出的快捷菜单中选择“操作主机”命令，如图 14-27 所示。

02 打开“操作主机”对话框，我们要做的就是将 RID、PDC、基础结构主机传送到服务器 B。首先单击“RID”选项卡，可以看到，当前操作主机是服务器 A 的计算机名 dc.msft.com，已经选中的是 AD.msft.com（服务器 B 的计算机名称），单击“更改”按钮（如图 14-28 所示），在弹出的对话框中，单击“是”按钮，确定传送操作主机角色，如图 14-29 所示。

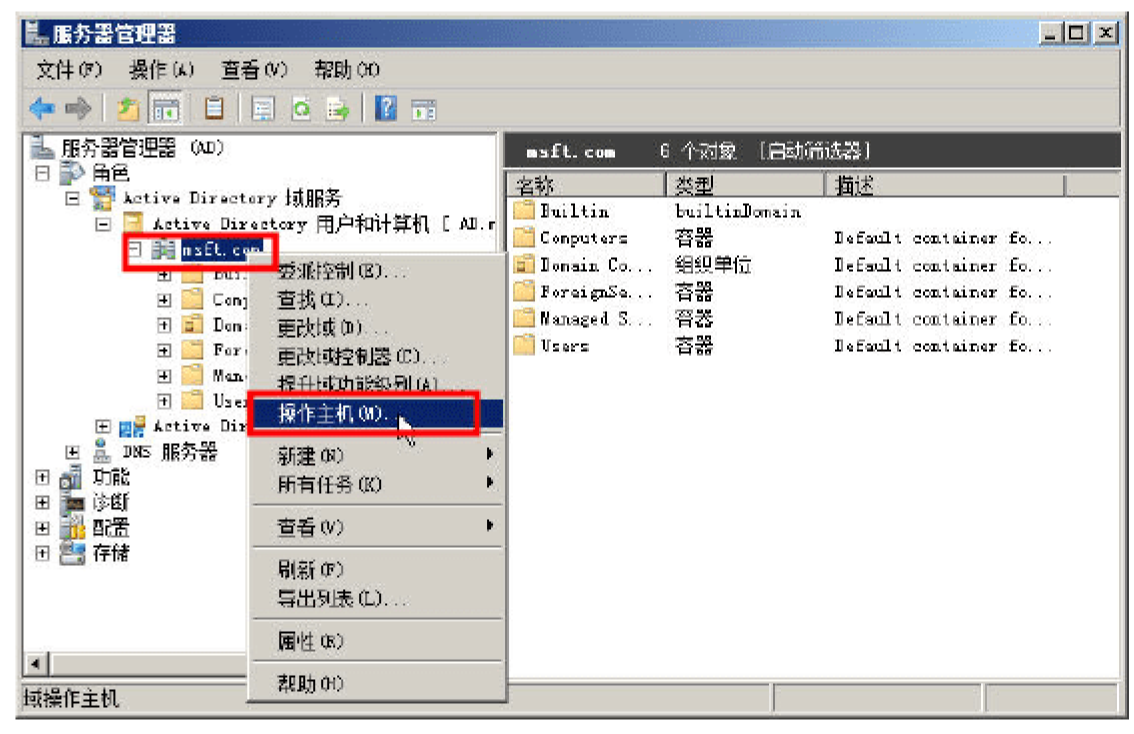


图 14-27　操作主机

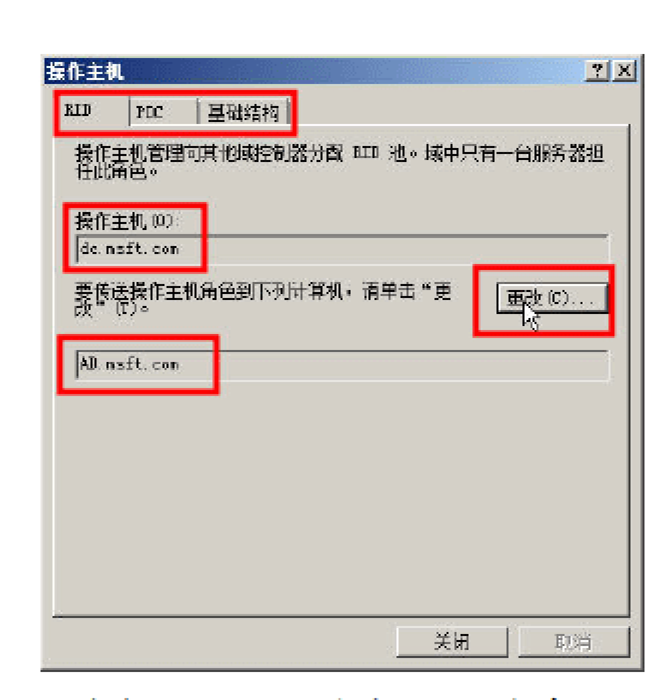


图 14-28　更改 RID 主机

03 然后单击“PDC”选项卡，单击“更改”按钮，如图 14-30 所示，传送 PDC 主机角色到 AD.mst.com。

04 最后在“基础结构”选项卡中，传送主机角色到 AD.msft.com，然后单击“关闭”按钮，完成操作主机的迁移，如图 14-31 所示。



图 14-29　确认传送

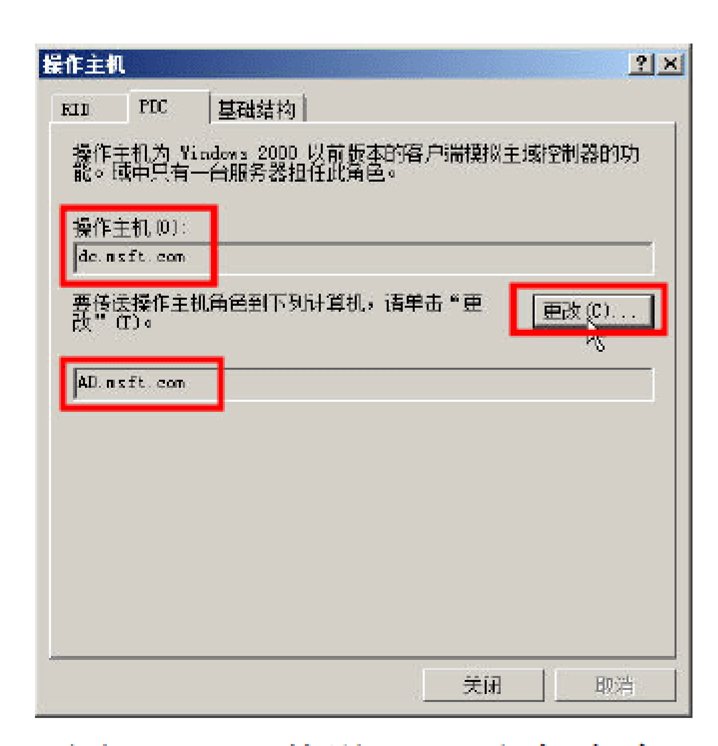


图 14-30　传送 PDC 主机角色

05 返回到“服务器管理器”控制台，右击域名，在弹出的快捷菜单中选择“更改域控制器”命令，如图 14-32 所示。

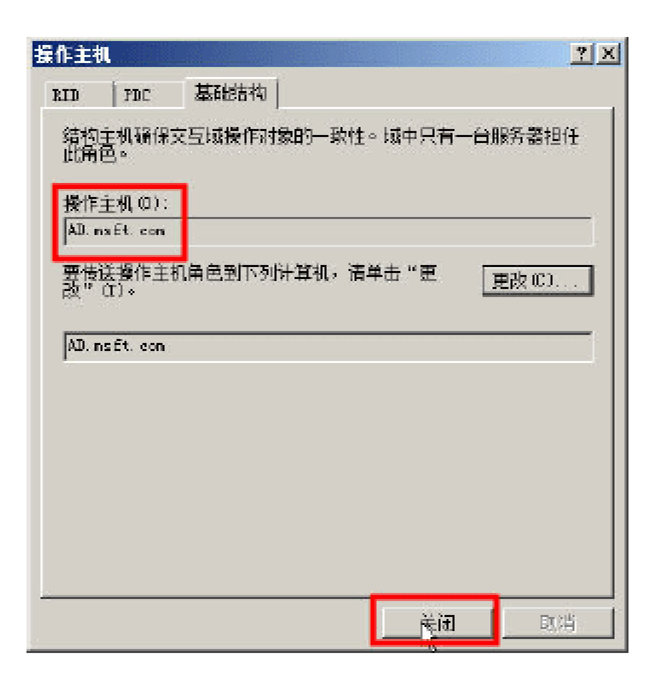


图 14-31　完成操作主机的迁移

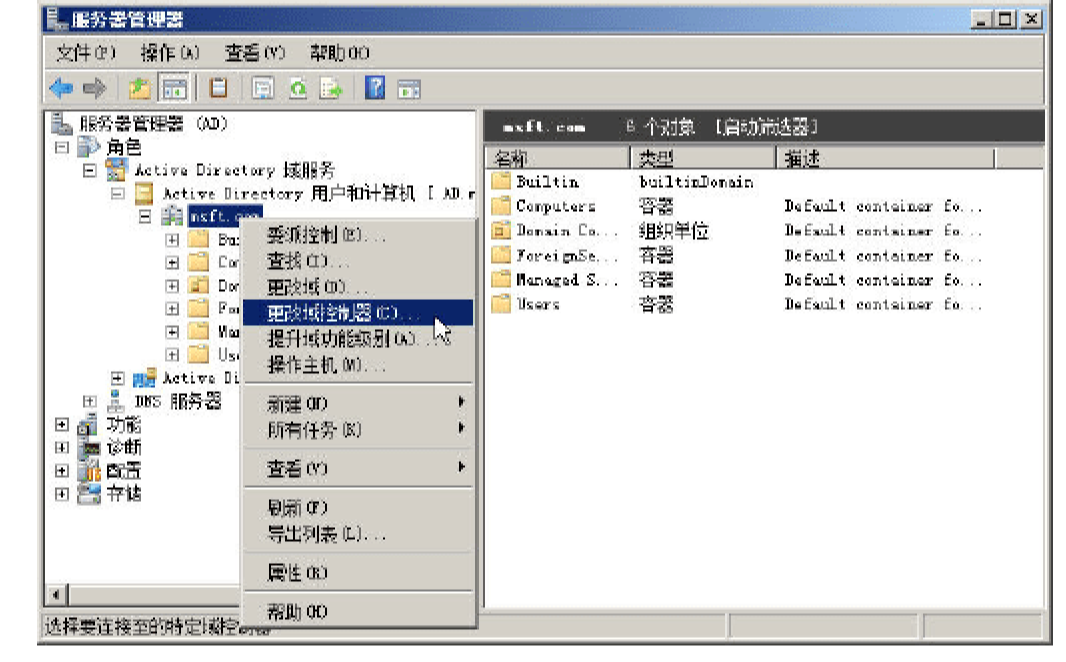


图 14-32　更改域控制器

06 在“更改目录服务器”对话框中，选中服务器 B 的计算机名称 AD.msft.com，然后单击“确定”按钮，如图 14-33 所示。

07 最后，修改服务器 B 的 IP 地址，将 DNS 地址改为服务器 B 的 IP 地址 192.168.80.11，如图 14-34 所示。

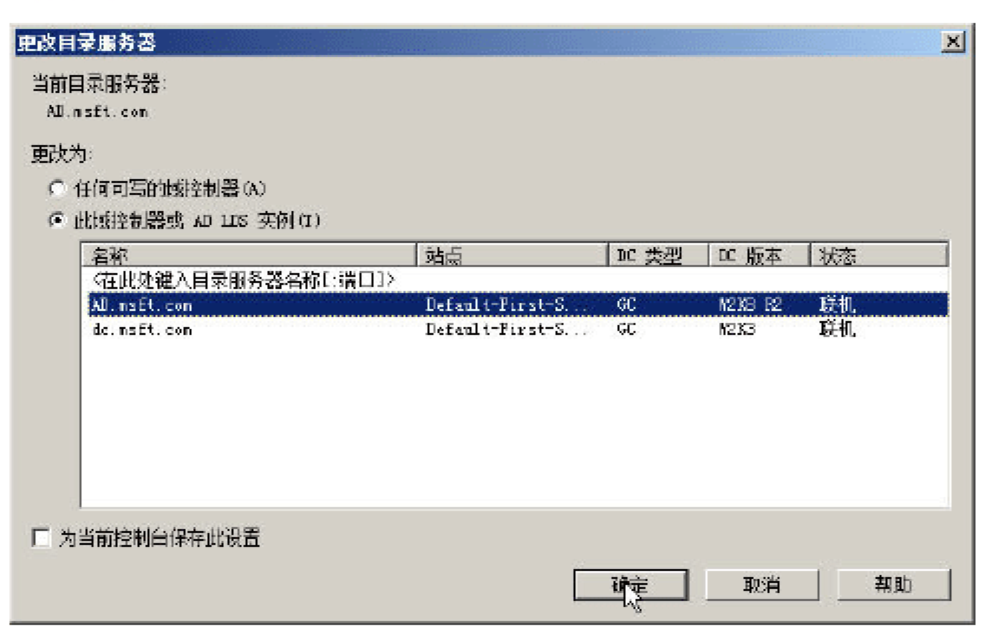


图 14-33　更改目录服务器

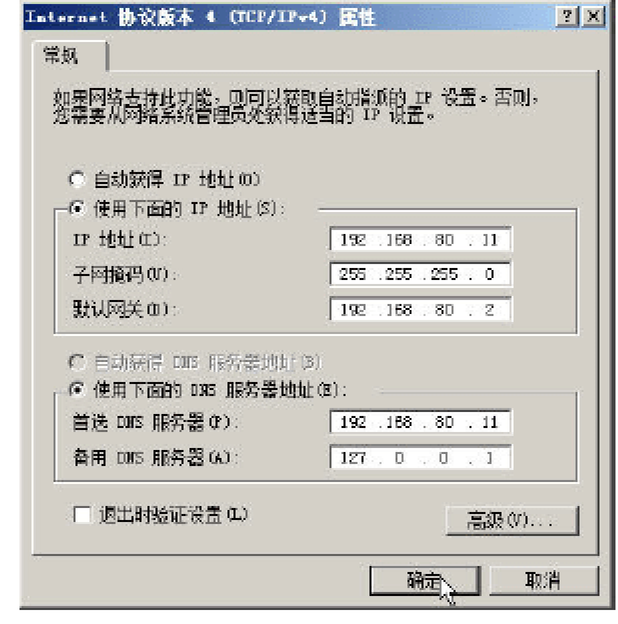


图 14-34　修改 DNS 地址

14.3.4　将原服务器 A 从 Active Directory 中脱离

在将服务器 B 升级到“主域控制器”之后，原服务器 A 将降级为“额外域控制器”。接下来的操作，是将服务器 A 从 Active Directory 中脱离，步骤如下。

01 切换到服务器 A 中，设置 DNS 地址为服务器 B 的 IP 地址 192.168.80.11，如图 14-35 所示。

02 运行 dcpromo，进入“Active Directory 安装向导”，在“删除 Active Directory”对话框中，单击“下一步”按钮，如图 14-36 所示。

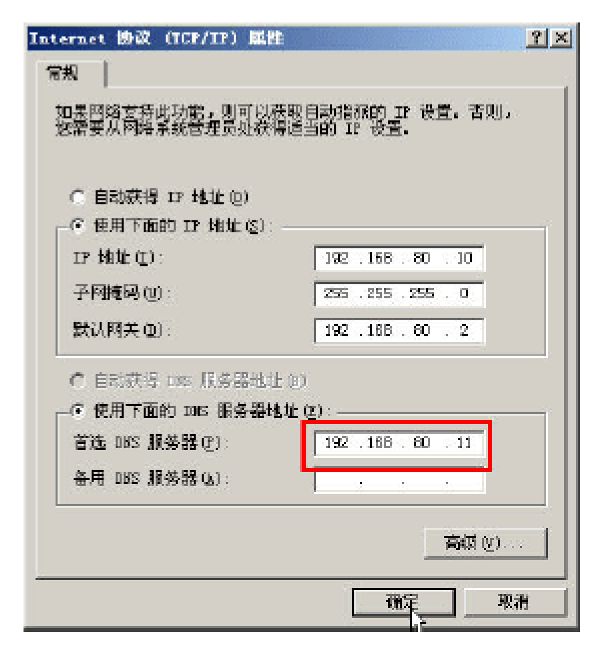


图 14-35　修改 DNS 地址

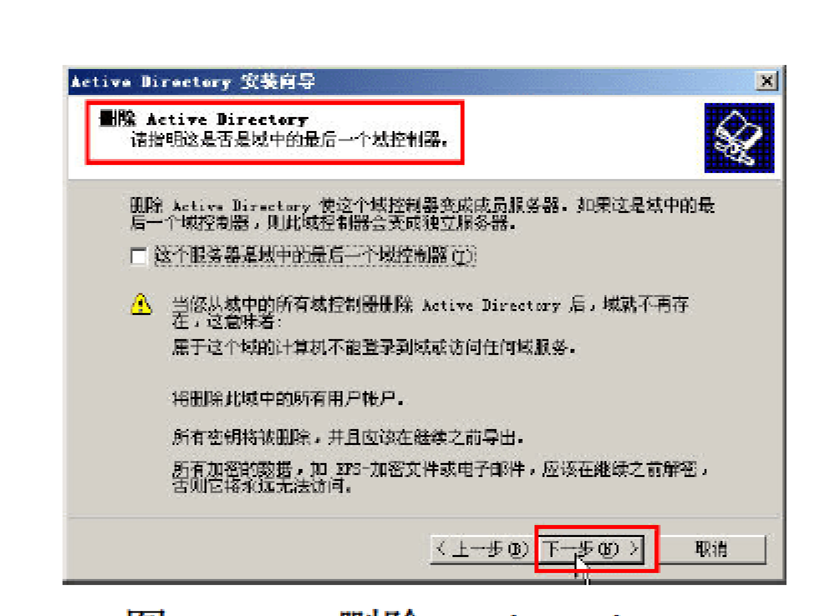


图 14-36　删除 Active Directory



说 明

不要选中“这个服务器是域中的最后一个域控制器”复选框，因为当前网络中还有一个域控制器。

03 在“管理员密码”对话框中，为脱离域的服务器，设置新的密码，如图 14-37 所示。

04 在“摘要”对话框中，复查并确认选定的选项，无误之后单击“下一步”按钮，如图 14-38 所示。

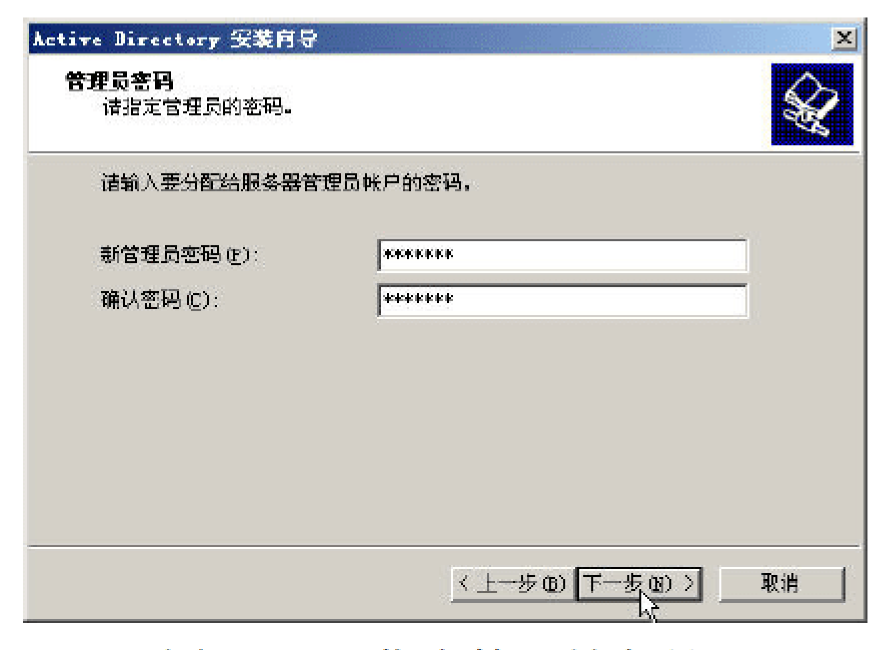




图 14-37 指定管理员密码

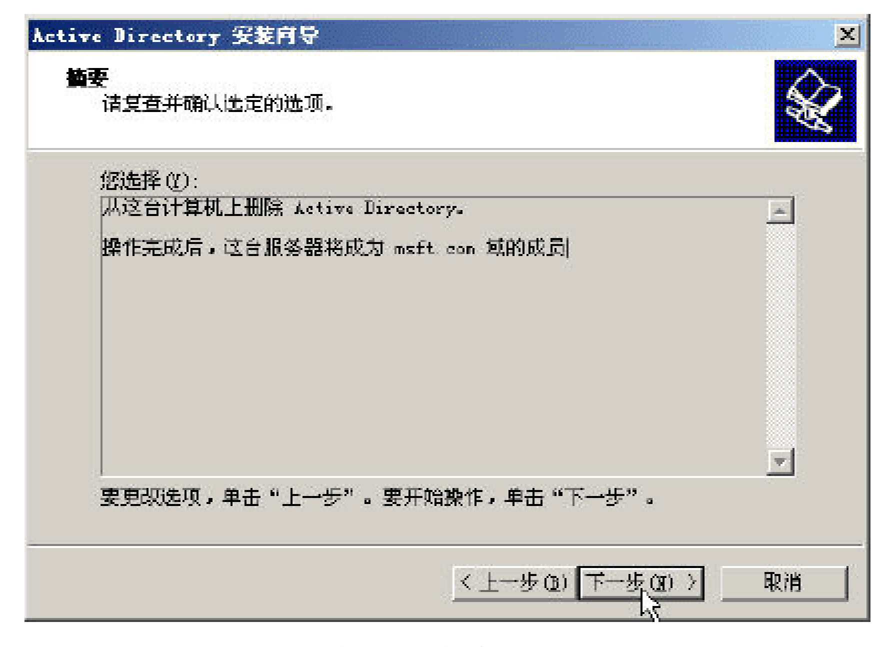


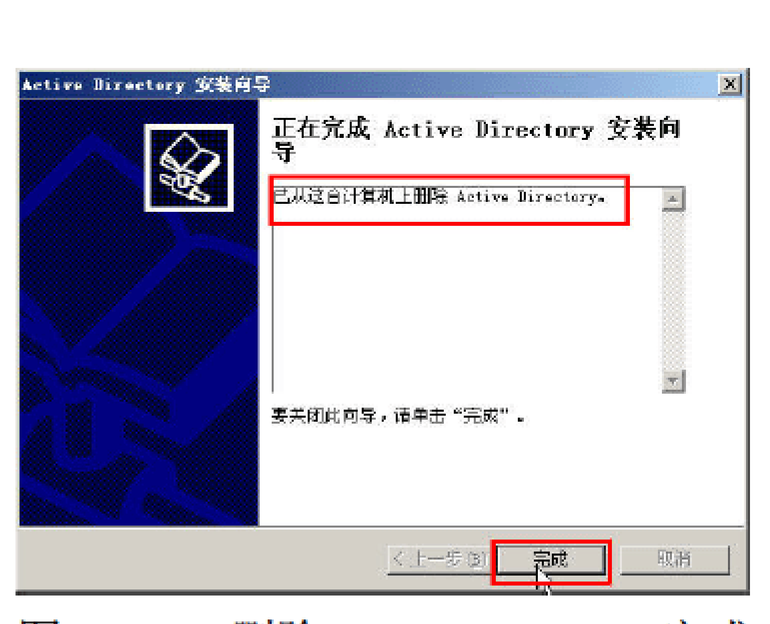
图 14-38 确认删除 Active Directory

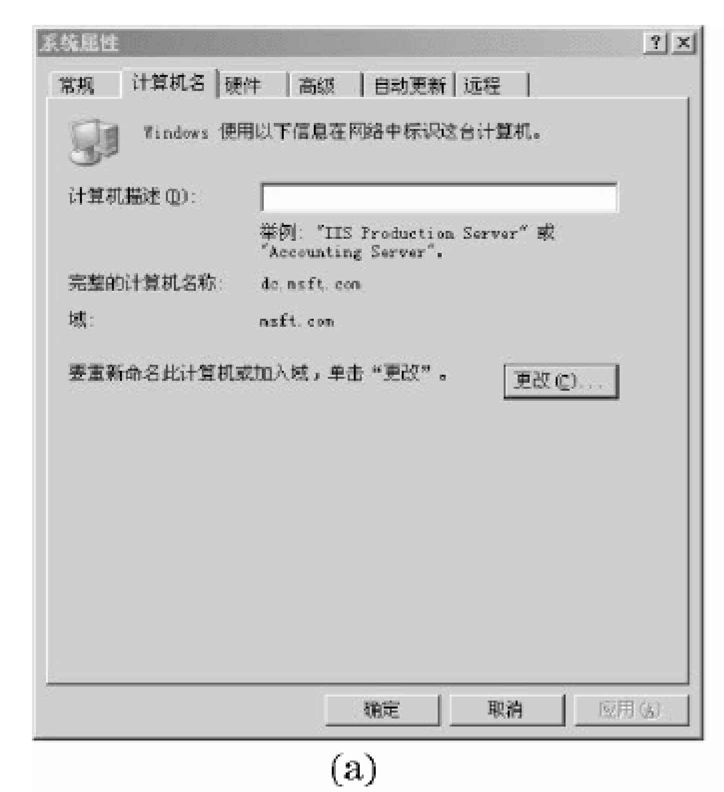
05 在“正在完成 Active Directory 安装向导”对话框中，显示“已从这台计算机上删除 Active Directory”，单击“完成”按钮，如图 14-39 所示。

06 在删除 Active Directory 完成之后，根据提示重新启动计算机。

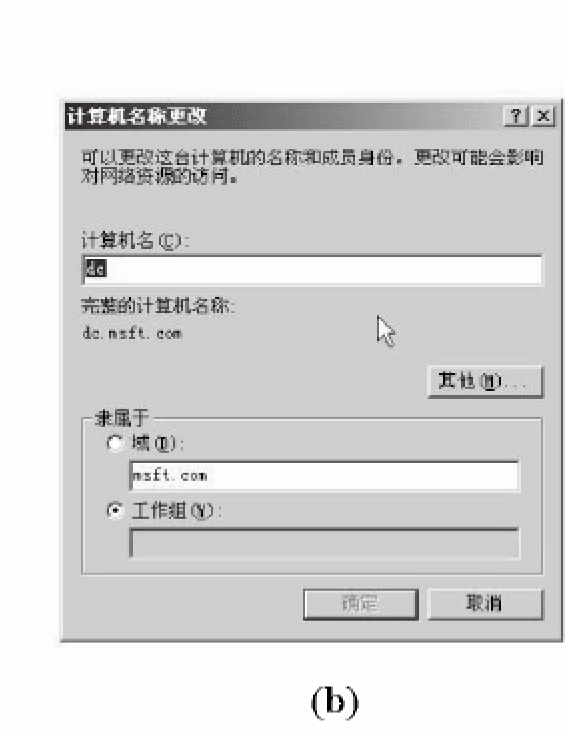
07 再次进入系统之后，打开“系统属性”，可以看到，当前的计算机已经是加入到 msft.com 中的一个“成员服务器”，如图 14-40（a）所示。

08 在图 14-40（b）所示的“计算机名称更改”对话框中，在“隶属于”选项组中，选中“工作组”单选按钮，将该计算机从 Active Directory 中脱离。脱离之后，重新启动计算机，至此，将计算机 A 从 Active Directory 中降级并脱离的步骤完成。





(a)



(b)

图 14-39 删除 Active Directory 完成

图 14-40 成员服务器

如果服务器 A 不符合安装 Windows Server 2008 或 Windows Server 2008 R2 的条件，则中间服务器 B 将代替服务器 A 对网络提供服务，此时，可以将服务器 A 关机，或者修改 IP 地址，以供他用。而服务器 B，则修改成原来服务器 A 的 IP 地址 192.168.80.10（DNS 地址亦修改为 192.168.80.10），

对原有网络提供服务。

14.3.5 在原服务器 A 上全新安装 Windows Server 2008 并完成迁移

如果原服务器 A 符合全新安装 Windows Server 2008 或 Windows Server 2008 R2 的条件，则可以在该服务器上，通过重新分区、格式化等操作安装 Windows Server 2008，并加入到域成为额外域控制器，然后升级到主域控制器，最后原服务器 B 降级，从域中脱离，即可完成整个升级步骤，这些步骤前面已经介绍过，不一一介绍。当然，也可以在服务器 A 成为主域控制器后，B 服务器降级成额外域控制器，但不从域中脱离，而成为额外域控制器，来对整个网络提供服务，这也是一种方法。

14.4 升级 ISA Server 到 Forefront TMG 2010

在前面介绍的内容，只是涉及到了 Active Directory 的升级，在实际的网络中，如果网络中有其他服务器，例如加入到 Active Directory 的 ISA Server、Windows Server 2003 中的 DHCP 服务器，要先完成这些服务器的升级，才能将整个网络升级到 Windows Server 2008 的 Active Directory。本节将介绍这两方面产品的升级。

ISA Server 只能安装在 Windows Server 2003 系统上，不能安装在 Windows Server 2008 操作系统上，而 Forefront TMG 2010 只能安装在 Windows Server 2008 X64 操作系统上，所以，不能从 ISA Server 2006 直接升级到 Forefront TMG 2010。要想完成从 ISA Server 2006 到 Forefront TMG 2010 的升级，只能先导出 ISA Server 2006 的策略，重新安装 Windows Server 2008、Forefront TMG 2010，再导入 ISA Server 2006 的策略，完成升级。

下面介绍从 ISA Server 2006 升级到 Forefront TMG 2010 的主要过程。

14.4.1 导出 ISA Server 2006 的策略

在 ISA Server 2006 中，可以根据需要导出 ISA Server 2006 的策略，主要有配置消息：包括 ISA Server 的所有配置，即 ISA Server 的防火墙策略、VPN 策略等。

- ISA Server 防火墙策略：包括 ISA Server 的所有防火墙策略。
- VPN 策略：包括 VPN 站点、VPN 服务器的策略。

如果要使升级后的 Forefront TMG 与原来有相同的配置，则可以选择导出 ISA Server 的策略；当然也可以同时导出防火墙策略与 VPN 策略。

1. 导出配置

在 ISA Server 中，导出配置的操作步骤如下。

01 在 ISA Server 2006 中，右击 ISA Server 的计算机名称，导出 ISA Server 2006 的备份，如

图 14-41 所示。

02 在“导出首选项”对话框中，选中“导出机密信息”与“导出用户权限设置”复选框，并且设置保护密码，如图 14-42 所示。



图 14-41　导出备份　　　图 14-42　导出首选项



说 明

一定要选中“导出机密信息”复选框，否则在 TMG2010 中将不能导入该设置。

03 指定导出文件位置，如图 14-43 所示。

04 导出完成，如图 14-44 所示。

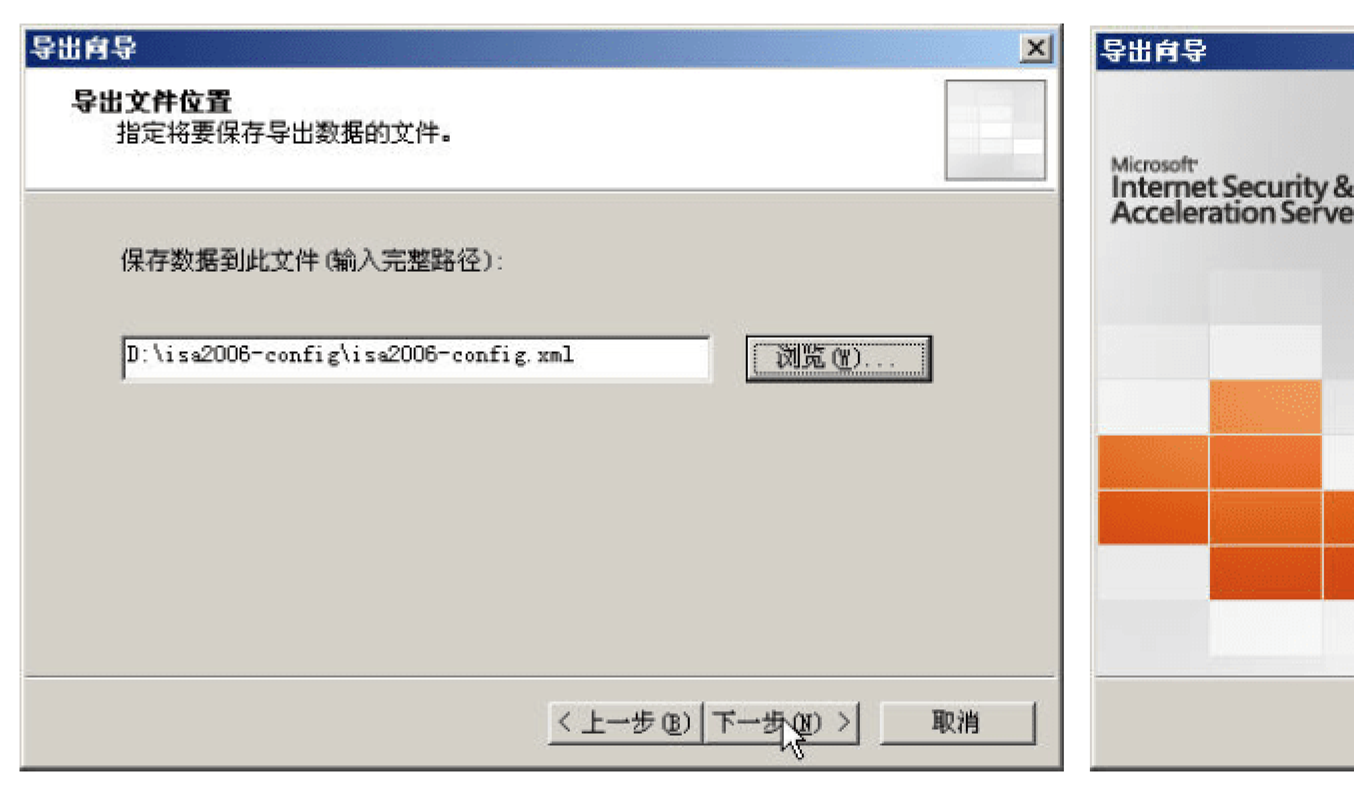


图 14-43　指定导出位置及文件名　　　图 14-44　导出设置完成

2. 导出防火墙策略

一般情况下，导出服务器的配置就可以了。也可以在“防火墙策略”中，只导出防火墙策略，这样只保留防火墙策略。如图 14-45 所示。

当然，在“导出首选项”对话框中，也要选中“导出机密信息”复选框，如图 14-46 所示。

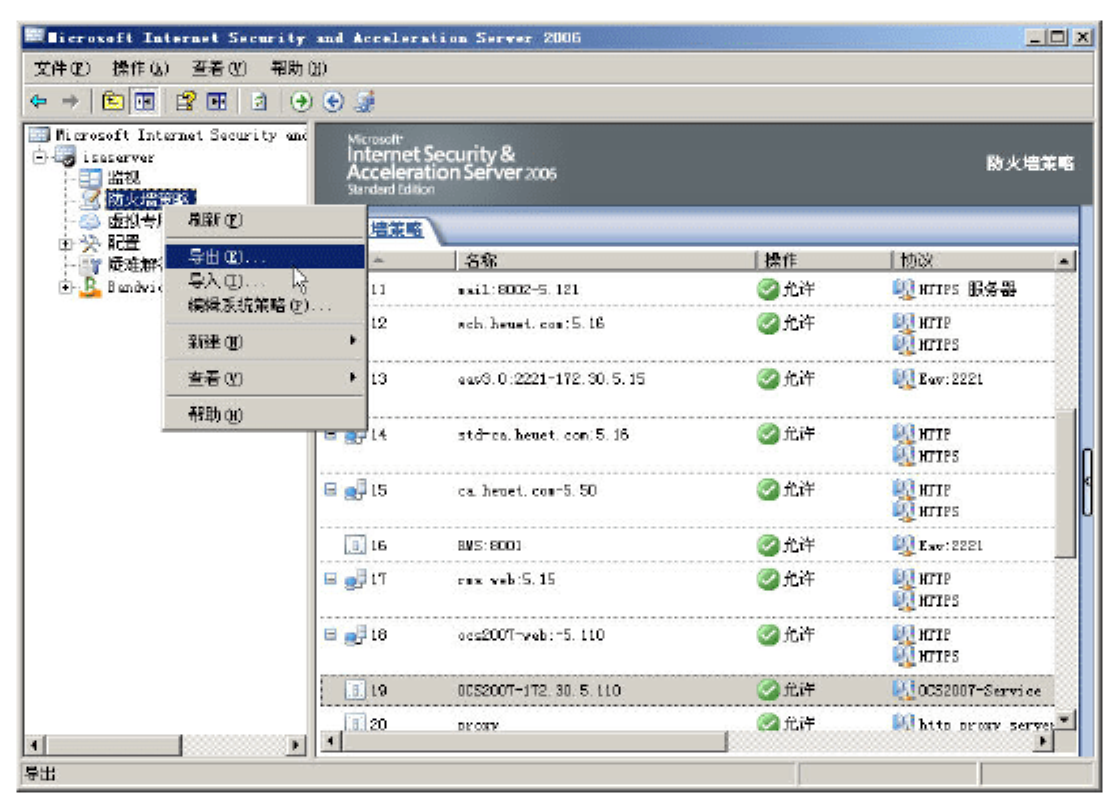


图 14-45　导出防火墙策略

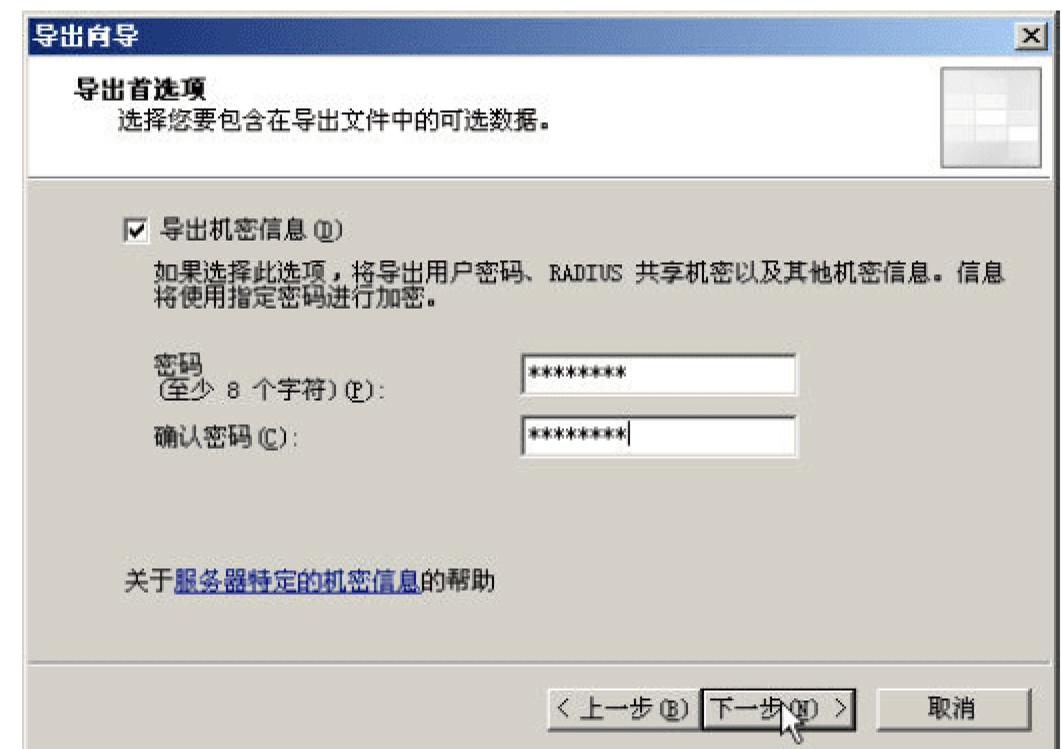


图 14-46　导出机密信息

3. 导出 VPN 客户端配置

也可以在“虚拟专用网”中，导出 VPN 配置。在使用这一项的时候，笔者竟然发现了 ISA Server 的一个“BUG”，如图 14-47 所示，这里面有两条命令都是“导出 VPN 客户端配置”，实际上第二项是“导入 VPN 客户端配置”。

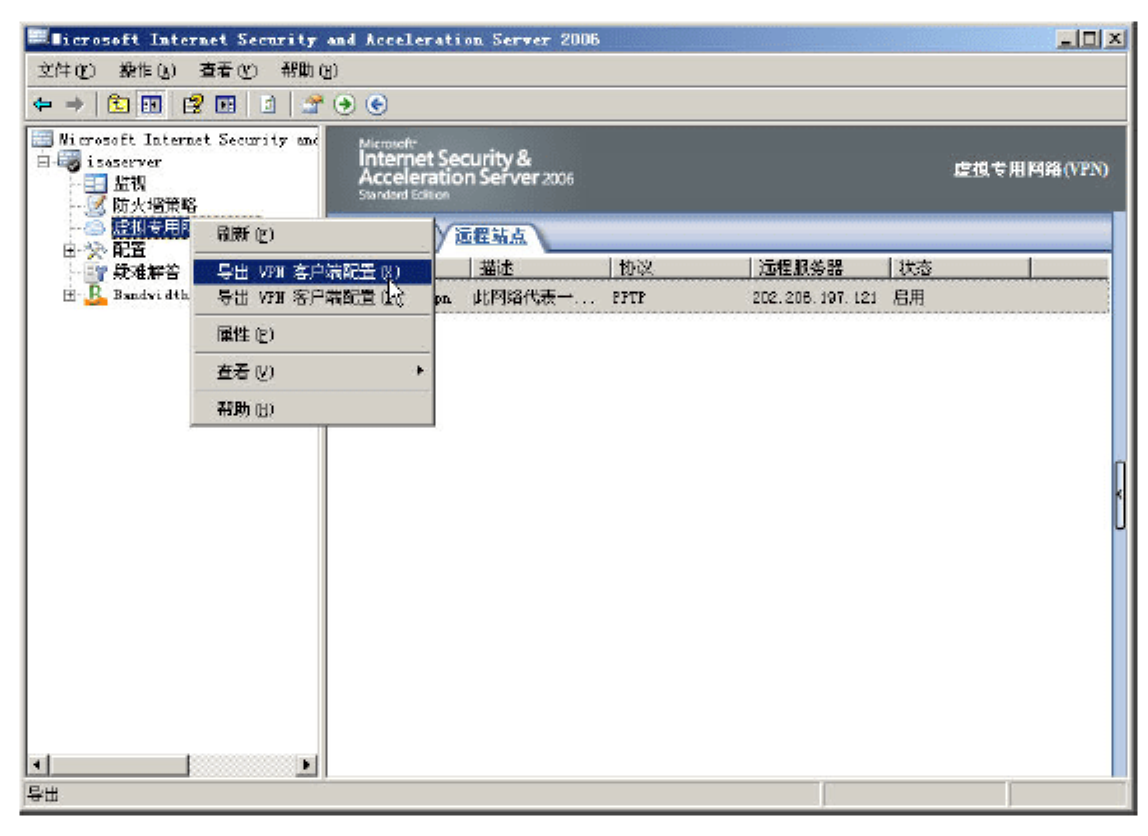


图 14-47　导出 VPN 客户端配置

14.4.2　在 TMG2010 中导入策略

将导出的 ISA Server 配置文件（或防火墙策略、VPN 客户端配置）复制到 TMG2010 计算机上，运行 TMG2010 管理控制台，导入 ISA Server 2006 的配置，主要步骤如下。

01 右击 TMG2010 计算机名称，在此可以导入原来 ISA Server 2006（或 TMG2010）的配置，如图 14-48 所示。如果要导入防火墙策略，则需要右击“防火墙策略”选项，而不是右击“计算机名称”选项。

02 选择导入文件，如图 14-49 所示。

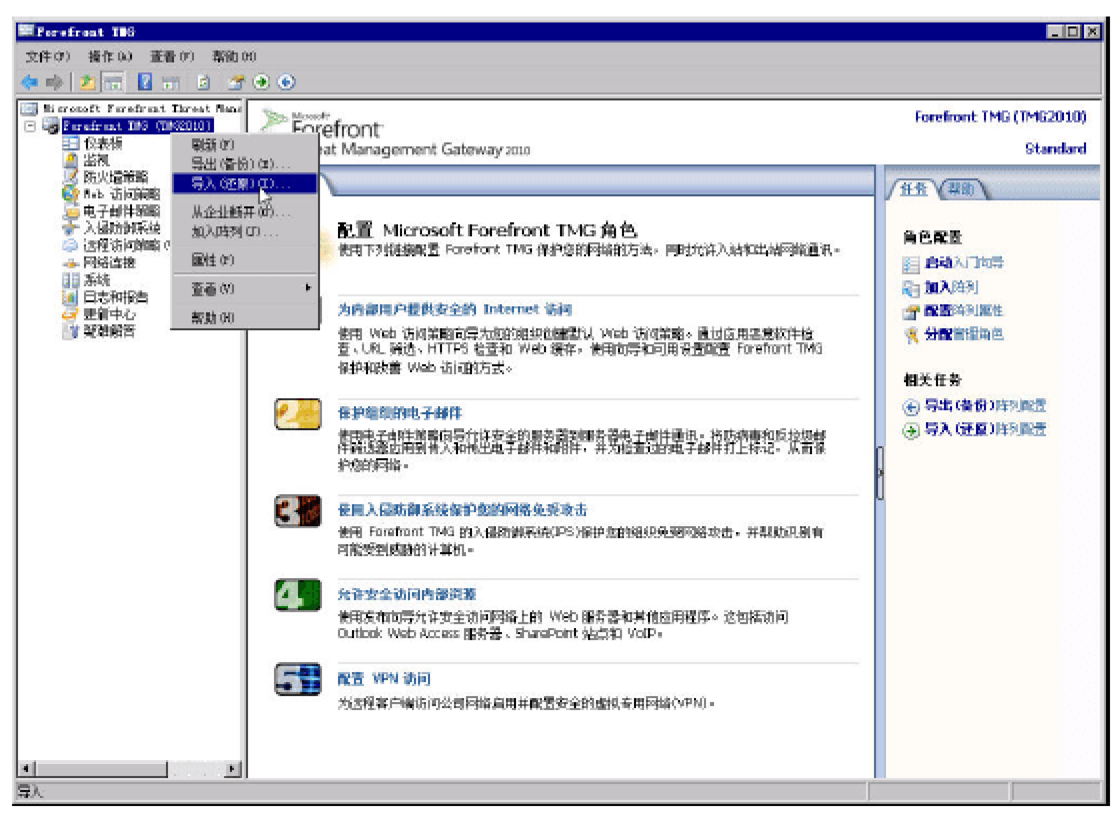


图 14-48　导入还原

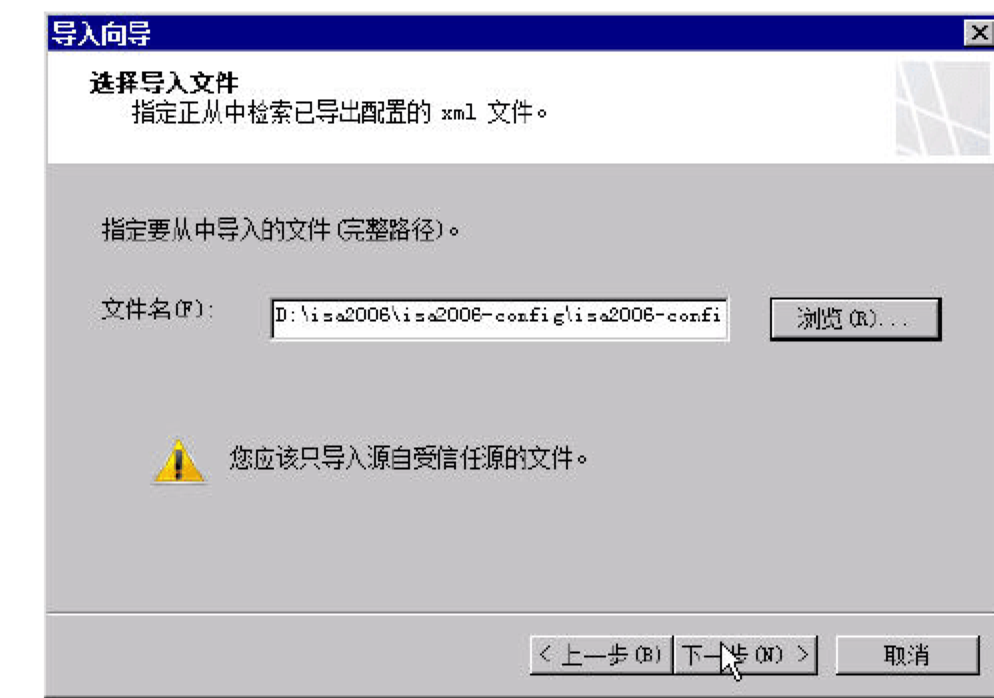


图 14-49　选择导入文件

03 此时会提示，你导入的是早期版本的 TMG 配置，单击“确定”按钮即可，如图 14-50 所示。

04 输入密码，这是在导出 ISA Server 2006 时所设置的，如图 14-51 所示。

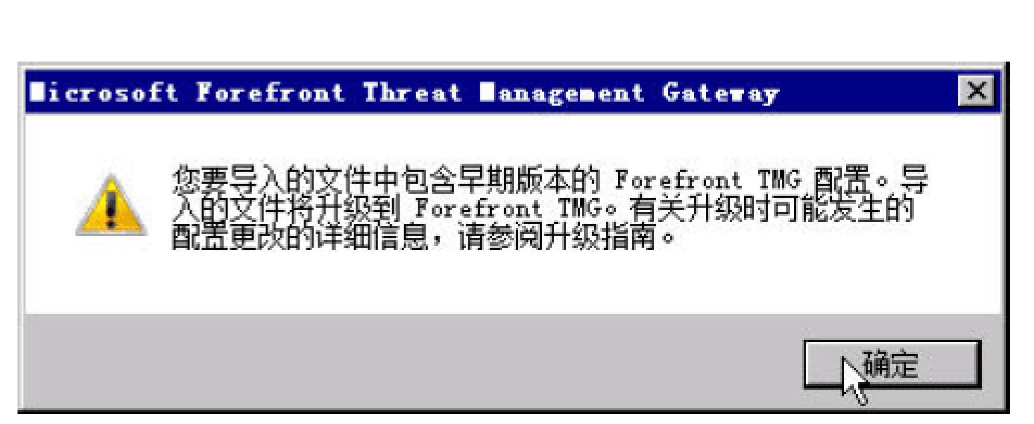


图 14-50　警告信息

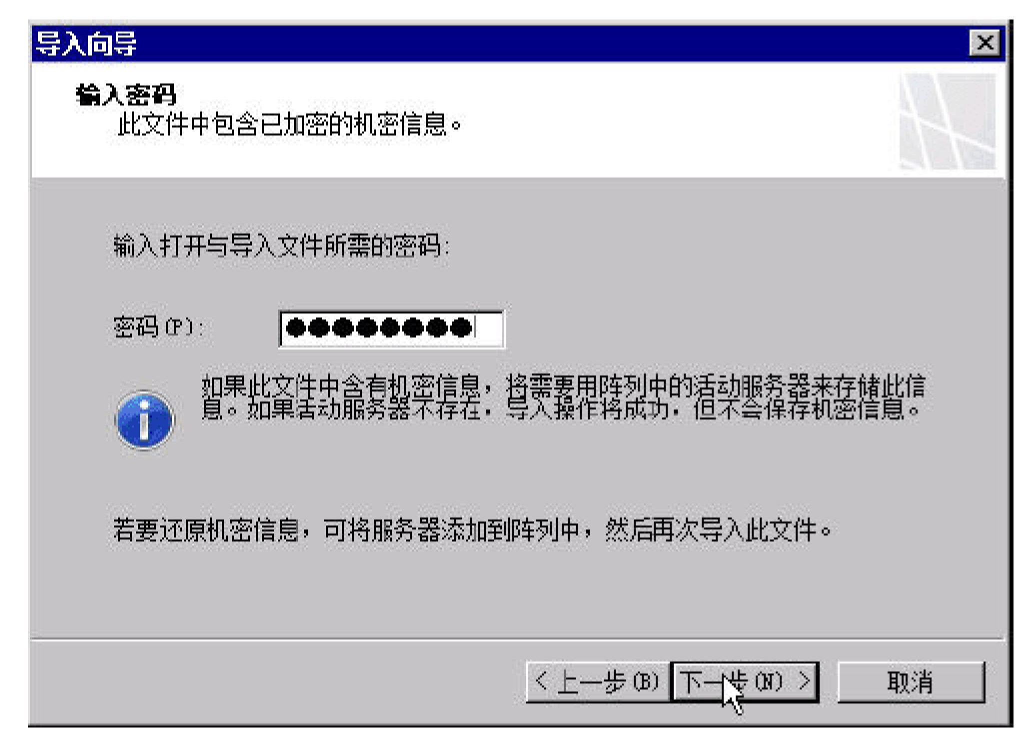


图 14-51　输入保护密码

05 如果在导出 ISA Server 配置时，没有选中“导出机密信息”选项，此时会弹出如图 14-52 所示的错误提示，并且不能继续操作。

06 导入完成，如图 14-53 所示。



图 14-52　无法导入

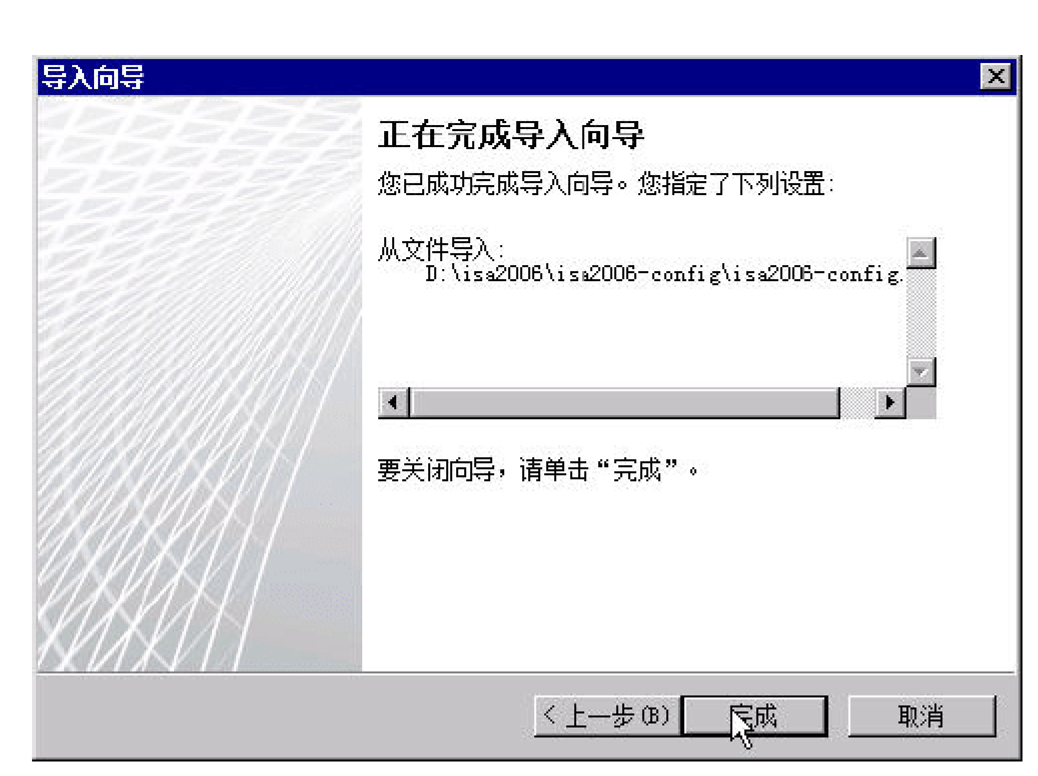


图 14-53　导入完成

07 导入配置完成后，单击“应用”按钮，让导入的配置生效，如图 14-54 所示。

08 如果原来的 ISA Server 提供了 VPN 或 VPN 路由功能，需要重新启动计算机，让 VPN 设置生效，如图 14-55 所示。

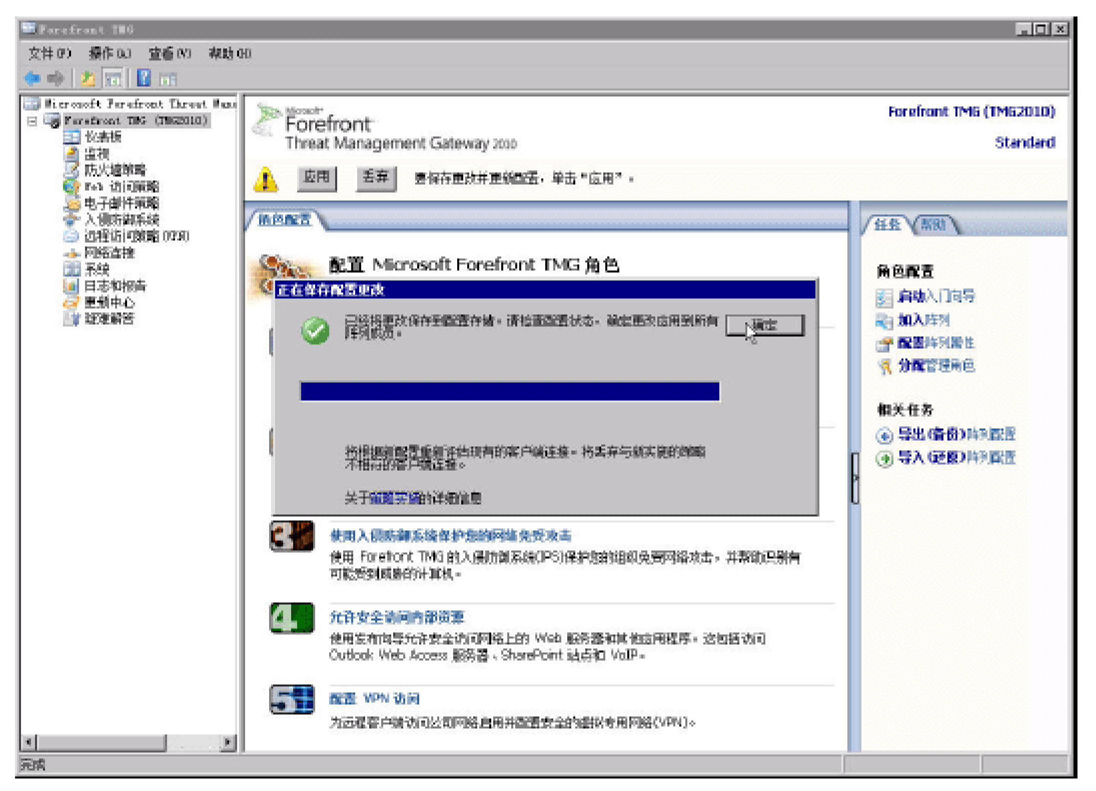


图 14-54 让配置生效

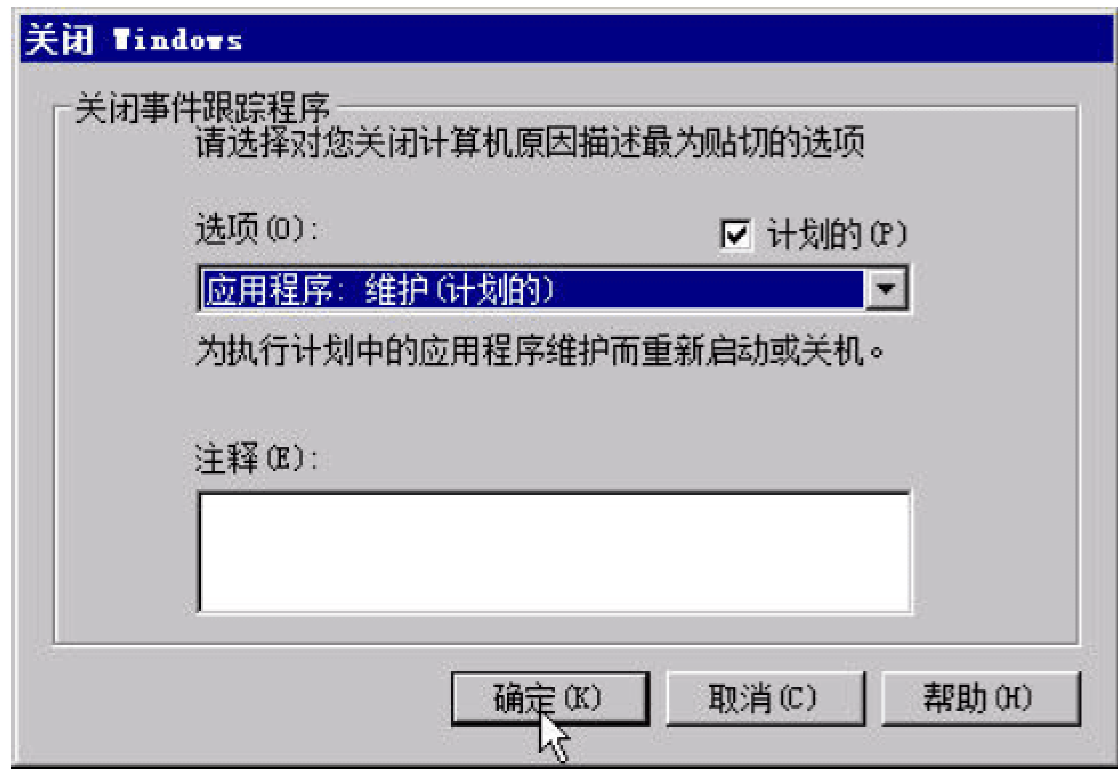


图 14-55 重新启动计算机

如果没有 VPN 配置，则不用重新启动计算机，当前导入的设置会立刻生效。

14.5 迁移 Windows Server 2003 的 DHCP 服务器到 Windows Server 2008 R2

在将 Windows Server 2003 升级到 Windows Server 2008 R2 的过程中，如果是通过“中间服务器”的方式升级，且网络中有 DHCP 服务器，则需要将 Windows Server 2003 的 DHCP 服务器的备份导出，在新的 Windows Server 2008 R2 中安装 DHCP 并将备份的数据导入，完成 DHCP 服务器的升级。下面通过具体的实例进行介绍。

网络中有 2 台 DHCP 服务器，这 2 台服务器都是安装的 Windows Server 2003，在升级到 Windows 2008 的过程中，其中 1 台计算机由于无法卸载 PowerShell 导致不能升级，另 1 台由于系统磁盘空间太小不能升级。因此只能是导出 DHCP 的配置，在网络中另 1 台计算机中安装 Windows Server 2008 R2 及 DHCP，并导入配置才可。在此简要介绍一下升级的步骤，其中原 Windows Server 2003 的 DHCP 服务器的 IP 地址是 172.30.5.9，新安装的 Windows Server 2008 R2 的 IP 地址是 172.30.5.15。

01 导出源 DHCP 数据库：在 172.30.5.9 的 Windows Server 2003 中，进入命令提示窗口执行下面语句：

```
netsh dhcp server dump > c:\exportdump.txt
```

02 导出目标 DHCP 数据：在 Windows Server 2008 R2 中安装 DHCP 服务器，进入命令提示窗口执行下面语句：

```
netsh dhcp server dump > c:\importdump.txt
```

然后将这个文件，复制到 172.30.5.9 的计算机上备用。

03 在 172.30.5.9 的计算机上，用“记事本”打开第 1 个导出文件，将

```
Dhcp Server 172.30.5.2 Add Class "默认路由和远程访问类别" "远程访问客户端的用户类别" 525241532e4d6963726f736f6674 0 b
Dhcp Server 172.30.5.2 Add Class "默认 BOOTP 的类别" "BOOTP 客户端的用户类别" 424f4f54502e4d6963726f736f6674 0 b
Dhcp Server 172.30.5.2 Add Class "Microsoft Windows 2000 选项" "Windows 2000 客户端的 Microsoft 供应商特定选项" 4d53465420352e30 1 b
Dhcp Server 172.30.5.2 Add Class "Microsoft Windows 98 选项" "Windows 98 客户端的 Microsoft 供应商特定选项" 4d534654203938 1 b
Dhcp Server 172.30.5.2 Add Class "Microsoft 选项" "适用于 Windows 98 和 Windows 2000 客户端的 Microsoft 供应商特定选项" 4d534654 1 b
```

这 5 行复制出来，另存为 1 个文件，并将其中的“Add”替换成“delete”，然后将“Dhcp”用“netsh dhcp”替换。

然后用“记事本”打开第 2 个导出文件，将

```
Dhcp Server \\Dhcp2008 Add Class "默认路由和远程访问类" "远程访问客户端的用户类" 525241532e4d6963726f736f6674 0 b
Dhcp Server \\Dhcp2008 Add Class "默认的网络访问保护级别" "受限访问客户端的默认特殊用户类" 4d53465420517561726616e74696e65 0 b
Dhcp Server \\Dhcp2008 Add Class "默认 BOOTP 类" "BOOTP 客户端的用户类" 424f4f54502e4d6963726f736f6674 0 b
Dhcp Server \\Dhcp2008 Add Class "Microsoft Windows 2000 选项" "针对 Windows 2000 及更高版本客户端的 Microsoft 供应商特定选项" 4d53465420352e30 1 b
Dhcp Server \\Dhcp2008 Add Class "Microsoft Windows 98 选项" "Windows 98 客户端的 Microsoft 供应商特定选项" 4d534654203938 1 b
Dhcp Server \\Dhcp2008 Add Class "Microsoft 选项" "适用于所有 Windows 客户端的 Microsoft 供应商特定选项" 4d534654 1 b
```

这 6 行复制出来，另存为 1 个文件，将其中的“\\Dhcp2008”用“172.30.5.2”替换，将“Dhcp”用“netsh dhcp”替换。其中“Dhcp2008”是 Windows Server 2008 的计算机名称。

然后将这 2 个文件中的内容，合并为 1 个新的文件，内容如下：

```
netsh dhcp Server 172.30.5.2 delete Class "默认路由和远程访问类别" "远程访问客户端的用户类别" 525241532e4d6963726f736f6674 0 b
netsh dhcp Server 172.30.5.2 delete Class "默认 BOOTP 的类别" "BOOTP 客户端的用户类别" 424f4f54502e4d6963726f736f6674 0 b
netsh dhcp Server 172.30.5.2 delete Class "Microsoft Windows 2000 选项" "Windows 2000 客户端的 Microsoft 供应商特定选项" 4d53465420352e30 1 b
netsh dhcp Server 172.30.5.2 delete Class "Microsoft Windows 98 选项" "Windows 98 客户端的 Microsoft 供应商特定选项" 4d534654203938 1 b
netsh dhcp Server 172.30.5.2 delete Class "Microsoft 选项" "适用于 Windows 98 和 Windows 2000 客户端的 Microsoft 供应商特定选项" 4d534654 1 b
netsh dhcp Server 172.30.5.2 Add Class "默认路由和远程访问类" "远程访问客户端的用户类" 525241532e4d6963726f736f6674 0 b
netsh dhcp Server 172.30.5.2 Add Class "默认的网络访问保护级别" "受限访问客户端的默认特殊用户类" 4d53465420517561726616e74696e65 0 b
```

```
netsh dhcp Server 172.30.5.2 Add Class "默认 BOOTP 类" "BOOTP 客户端的用户类" 424f4f54502e4d6963726f736f6674 0 b
netsh dhcp Server 172.30.5.2 Add Class "Microsoft Windows 2000 选项" "针对 Windows 2000 及更高版本客户端的 Microsoft 供应商特定选项" 4d53465420352e30 1 b
netsh dhcp Server 172.30.5.2 Add Class "Microsoft Windows 98 选项" "Windows 98 客户端的 Microsoft 供应商特定选项" 4d534654203938 1 b
netsh dhcp Server 172.30.5.2 Add Class "Microsoft 选项" "适用于所有 Windows 客户端的 Microsoft 供应商特定选项" 4d534654 1 b
```

并修改扩展名为“.bat”或“.cmd”。然后执行这个批处理文件，如图 14-56 所示。

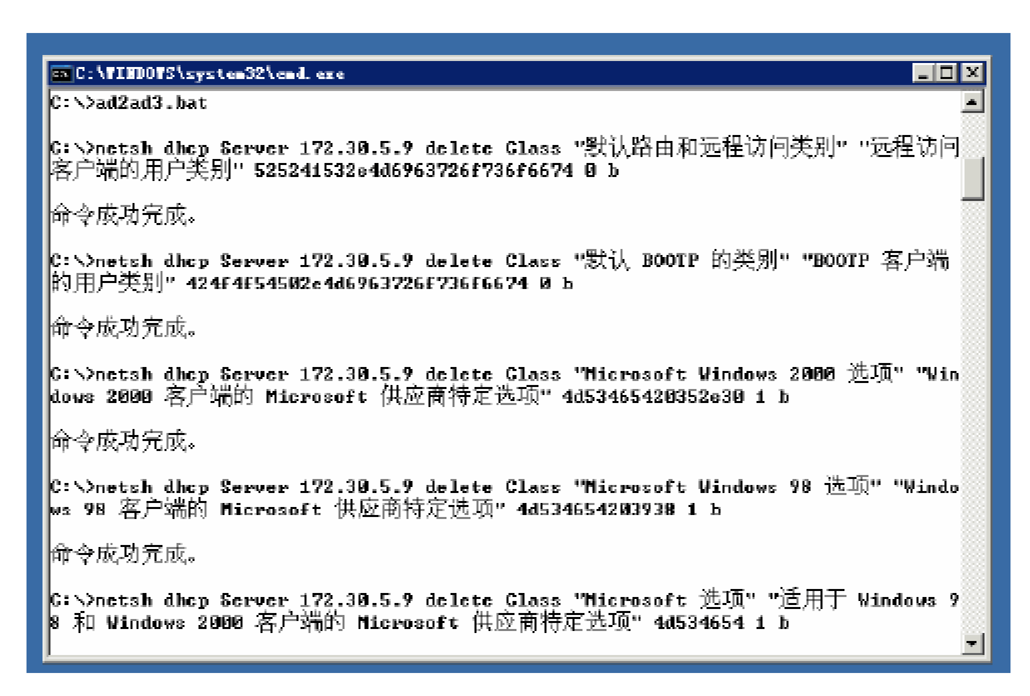


图 14-56　执行批处理文件

04 导出源 Windows 2003 的 DHCP 数据库：在 172.30.5.9 的计算机中执行下面语句：

```
netsh dhcp server export   c:\dhcp-172.30.5.9.txt   all
```

如图 14-57 所示。

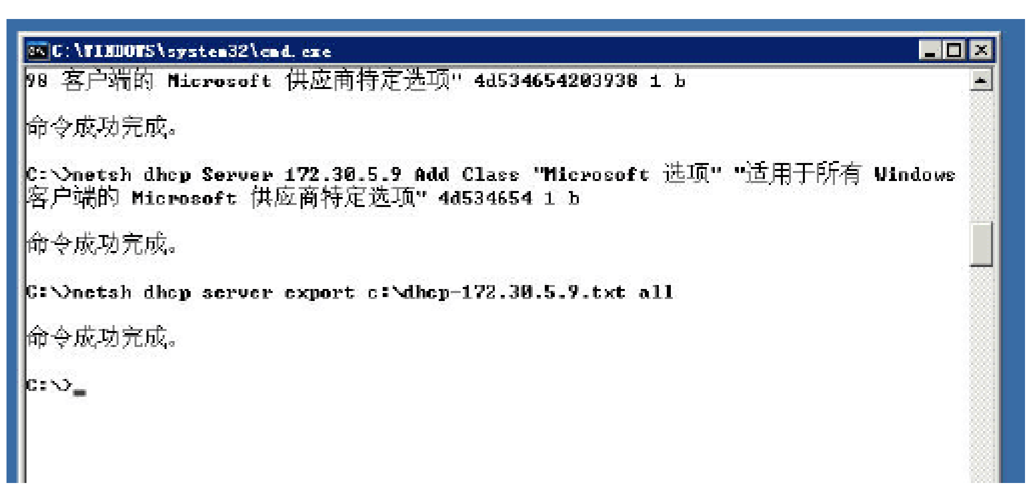


图 14-57　导出 Windows 2003 的 DHCP

05 导入 DHCP 数据库到 Windows Server 2008 R2 数据库中：复制上一步导出的文件到 172.30.5.15 的 Windows Server 2008 计算机，执行下面语句：

```
netsh dhcp server import c:\dhcp-172.30.5.9.txt
```

如图 14-58 所示。

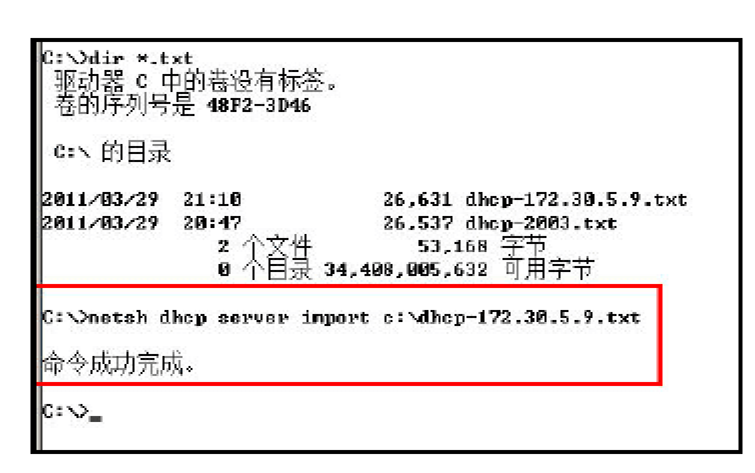


图 14-58　导入成功

06 打开 Windows Server 2008 的 DHCP，检查导入是否安装成功，如图 14-59 所示。

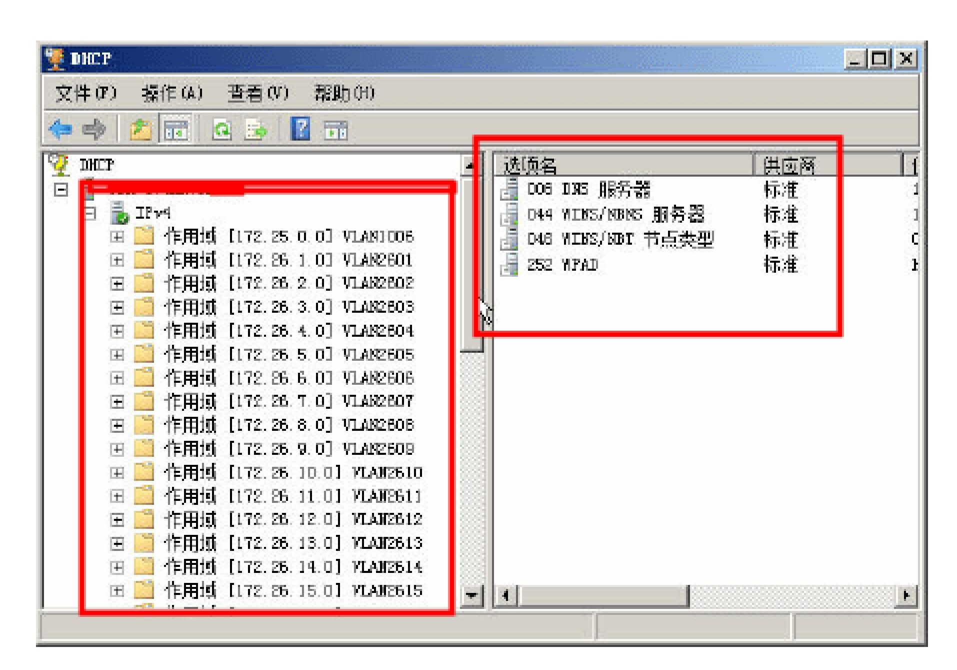


图 14-59 导入成功



说 明

如果要将 Windows Server 2003 的 DHCP，迁移到 Windows Server 2008 的 DHCP，只需要执行步骤 4～5 即可，不需要执行步骤 1～3。

第 15 章　使用网络为工作站部署操作系统

Windows 部署服务（Windows Deployment Services,WDS）是“RIS（远程安装）服务”的升级版本，它可以使用“Windows 映像（WIM）文件”为网络中的计算机，远程安装 Windows 操作系统。多台计算机可以同时安装，并且不需要安装盘，大大提高了操作系统的安装效率。Windows 部署服务可以用来安装 Windows Vista、Windows 7、Windows Server 2008 和 Windows Server 2008 R2 操作系统。

15.1　什么是 Windows 部署服务

Windows 部署服务是 Windows 远程安装服务（RIS）的升级版本，它能为用户计算机远程安装操作系统而无须物理上接触每个用户机器。使用 Windows 部署服务可以通过 Windows 映像（wim）文件安装 Windows 操作系统，它支持初始安装，也可以在现有计算机上重新安装操作系统。尤其是可以在连接网络的计算机上，通过网络远程启动计算机，使用一个有效的账户进行登录，即可通过远程服务器的 Windows 部署服务重新部署操作系统。

Windows 部署服务具有以下优势：

- 降低部署的复杂程度以及与手动安装效率低下关联的成本。
- 允许基于网络安装 Windows 操作系统（包括 Windows Vista、Windows 7 和 Windows Server 2008、Windows Server 2008 R2）。
- 将 Windows 映像部署到未安装操作系统的计算机上。
- 支持包 Windows Vista、Windows 7、Windows Server 2008、Windows Server 2008 R2、Windows XP 和 Windows Server 2003 的混合环境。
- 为把 Windows 操作系统部署到客户端计算机和服务器，提供端到端的解决方案。
- 基于标准的 Windows Server 2008 安装技术（包括 Windows PE、.wim 文件和基于映像的安装）。

Windows Server 2008 及 Windows Server 2008 R2 中部署服务的改进：

- 可以部署 Windows Vista、Windows 7 和 Windows Server 2008、Windows Server 2008 R2。
- 支持将 Windows PE 作为启动操作系统。

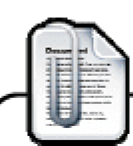
- 支持 Windows 映像（.wim）格式，不支持 RISETUP 映像和 OSChooser 屏幕。
- 可以使用多播功能传输数据和映像。
- 可以在独立服务器上使用多播功能传输数据和映像（在安装传输服务器角色服务时）
- 可扩展性能更高的 PXE 服务器组件。
- 用于选择启动操作系统的新启动菜单。
- 可以用于选择和部署映像，以及管理 Windows 部署服务服务器和客户端的新图形用户界面。
- 增强的 TFTP 服务器。
- 支持通过网络启动具有可扩展固件接口（EFI）的基于 x64 的计算机。
- 安装度量值报告。

15.2 Windows 部署服务的系统需求

无论是服务器还是客户端计算机，Windows 部署服务都未提出任何内存或 CPU 速度的要求。Windows 部署服务器需要使用 NTFS 文件系统分区，并为映像存储提供足够的磁盘空间，以容纳所有必需的映像。

Windows 部署服务要求下列操作系统：

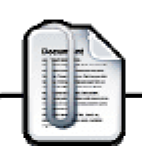
- Windows Server 2008、Windows Server 2008 R2。
- Windows Server 2003 Service Pack 1（SP1）。



说 明

目前已推出适用于 Windows Server 2003 SP1 的 Windows 部署服务更新包。必须安装远程安装服务（RIS），但无须对其进行配置。

- Windows Server 2003 Service Pack 2（SP2）。



说 明

如果已安装 RIS，Windows Server 2003 SP2 将默认安装 Windows 部署服务。

- Windows Server 2008 Service Pack 1（SP1）。

Windows 部署服务的环境必须满足下列要求：

- Windows 部署服务器必须是 Active Directory 域的成员。
- 必须具有 DHCP 服务器。
- 计算机必须支持 PXE 网络启动。

15.3 Windows 部署服务的安装

本节将在 Windows Server 2008 R2 企业版的计算机（已升级到 Active Directory 服务器）上安装“Windows 部署服务”，服务器配置为：计算机 IP 地址为 172.30.5.15、计算机名称为 DC、Active Directory 域名为 heinfo.local，Windows 部署服务的安装步骤如下。

01 选择“开始→程序→管理工具→服务器管理器”，打开“服务器管理器”控制台，选择“角色”选项，单击“添加角色”链接，运行“添加角色向导”。

02 在“选择服务器角色”对话框中，选中“Windows 部署服务”复选框，如图 15-1 所示。

03 在“选择角色服务”对话框中，选中“部署服务器”和“传输服务器”复选框，如图 15-2 所示。





图 15-1 选择服务器角色

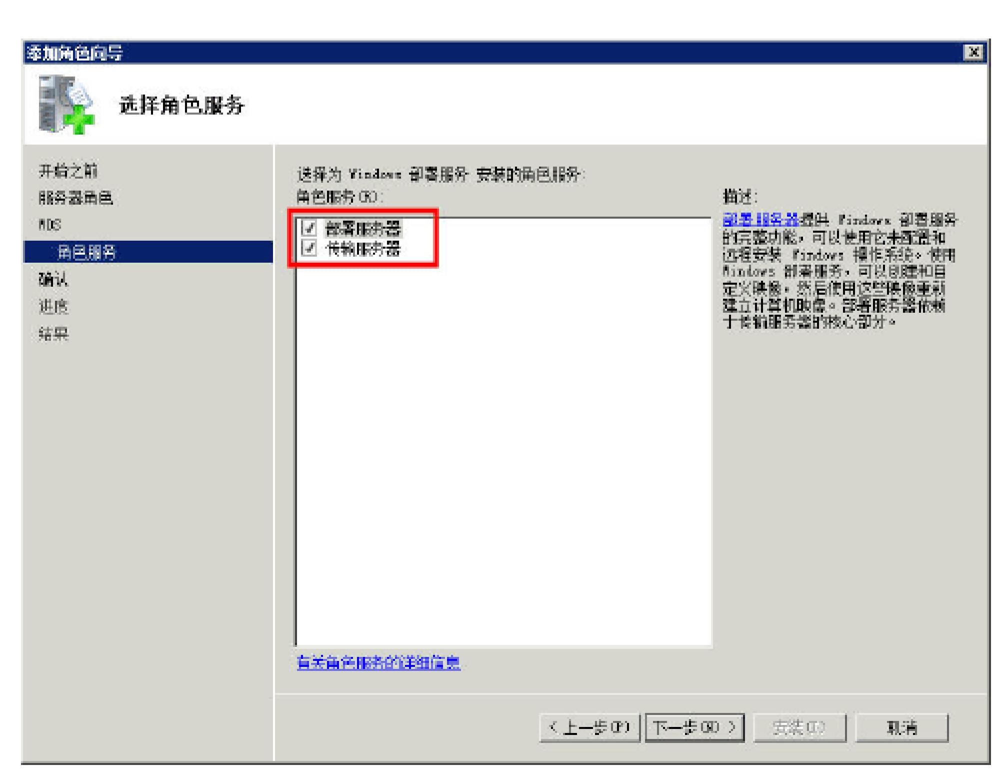


图 15-2 选择角色服务

04 在“确认安装选择”对话框中，查看并确认将要安装的角色或功能，如图 15-3 所示。

05 单击“安装”按钮开始安装。安装结束后，显示“安装结果”对话框，如图 15-4 所示。单击“关闭”按钮退出即可。



图 15-3 确认安装选择

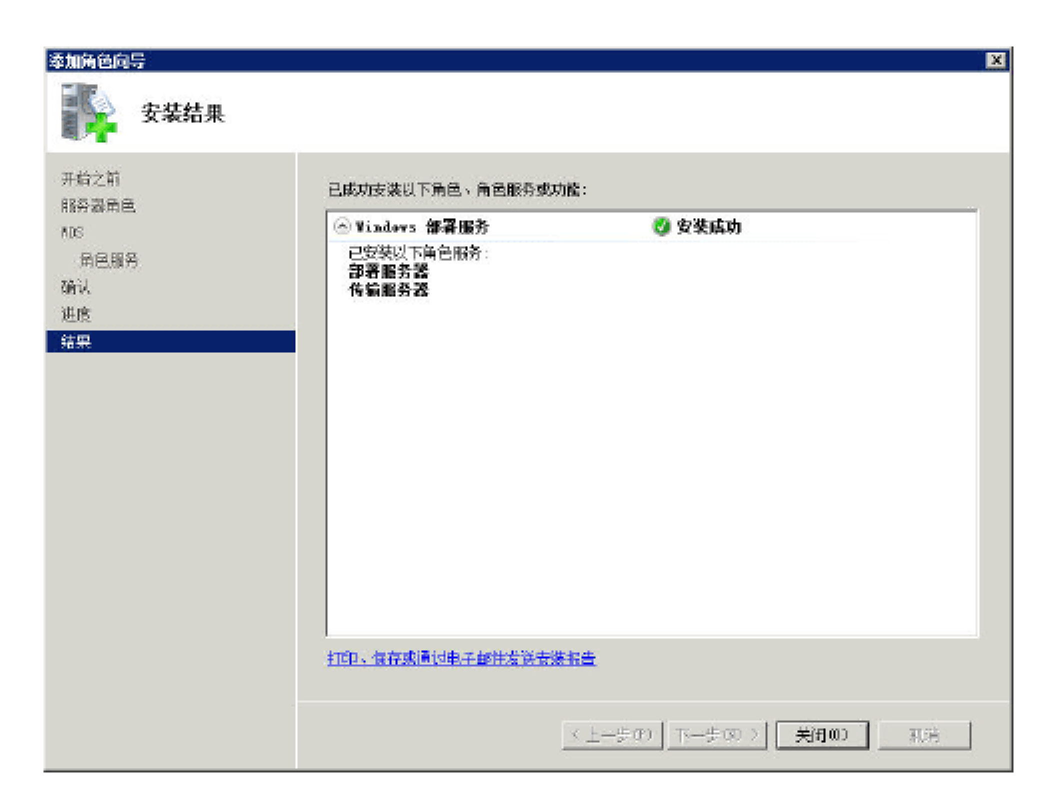


图 15-4 安装结果

如果你的 DHCP 服务器没有安装，可运行“添加角色向导”，添加“DHCP 服务器”。有关 DHCP

服务器的安装与配置，可参考本书第 3 章的内容，下面只介绍 DHCP 服务器的注意问题。

01 在“选择服务器角色”对话框中添加“DHCP 服务器”，如图 15-5 所示。

02 在“选择网络连接绑定”对话框中，选中“172.30.5.15”复选框，如图 15-6 所示。

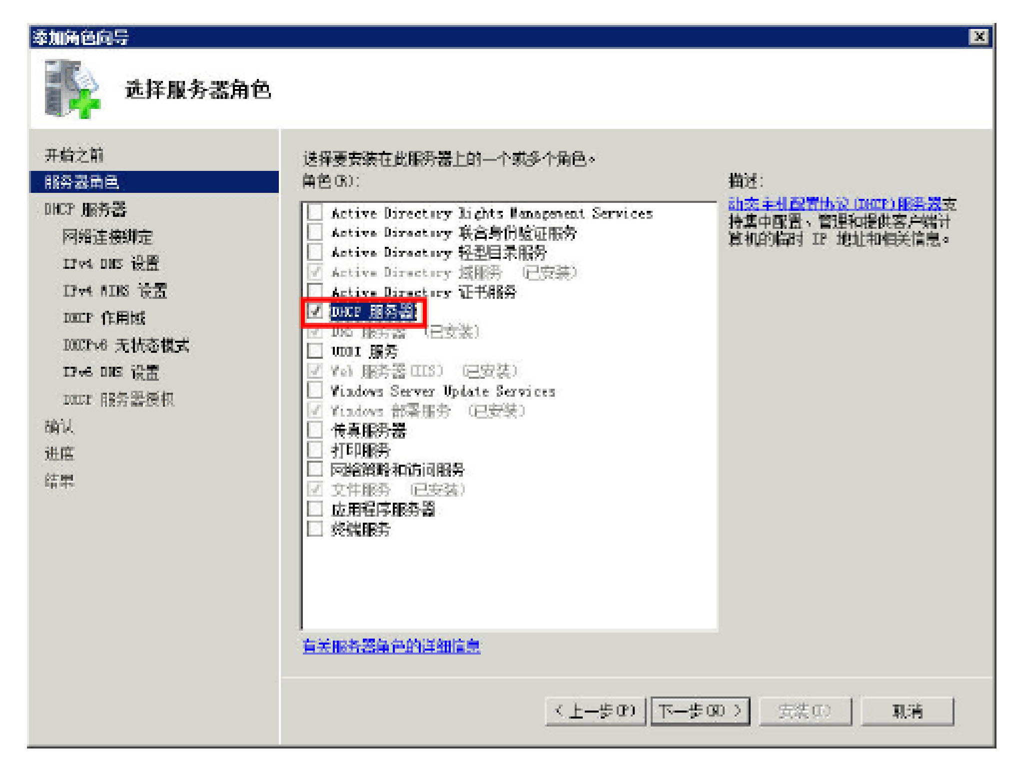


图 15-5　添加 DHCP 服务器

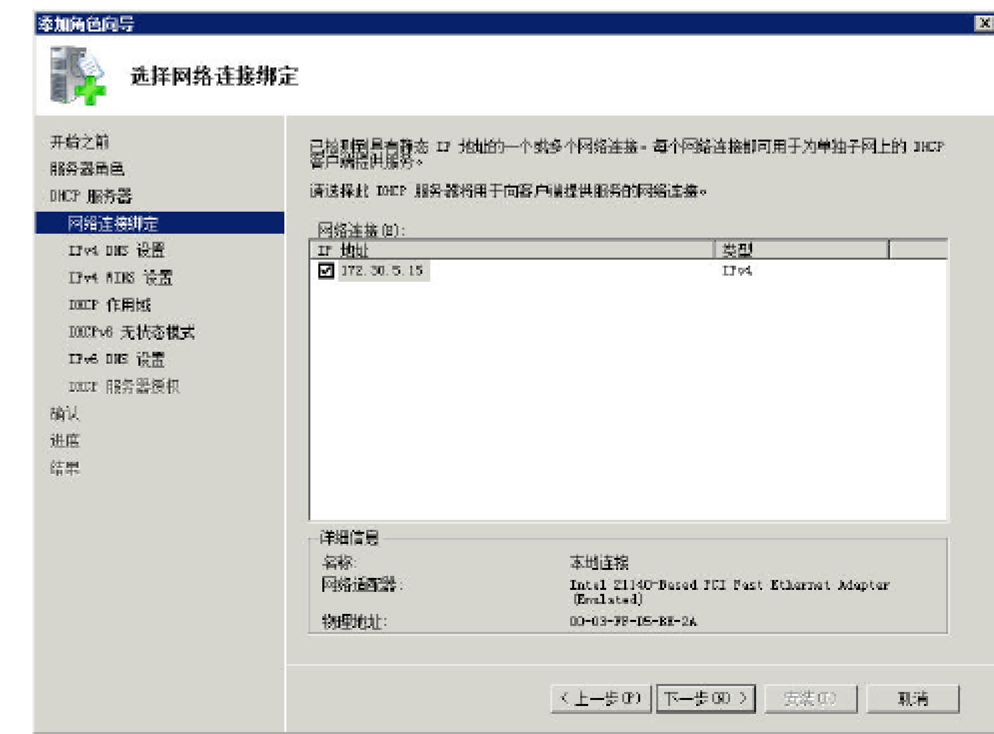
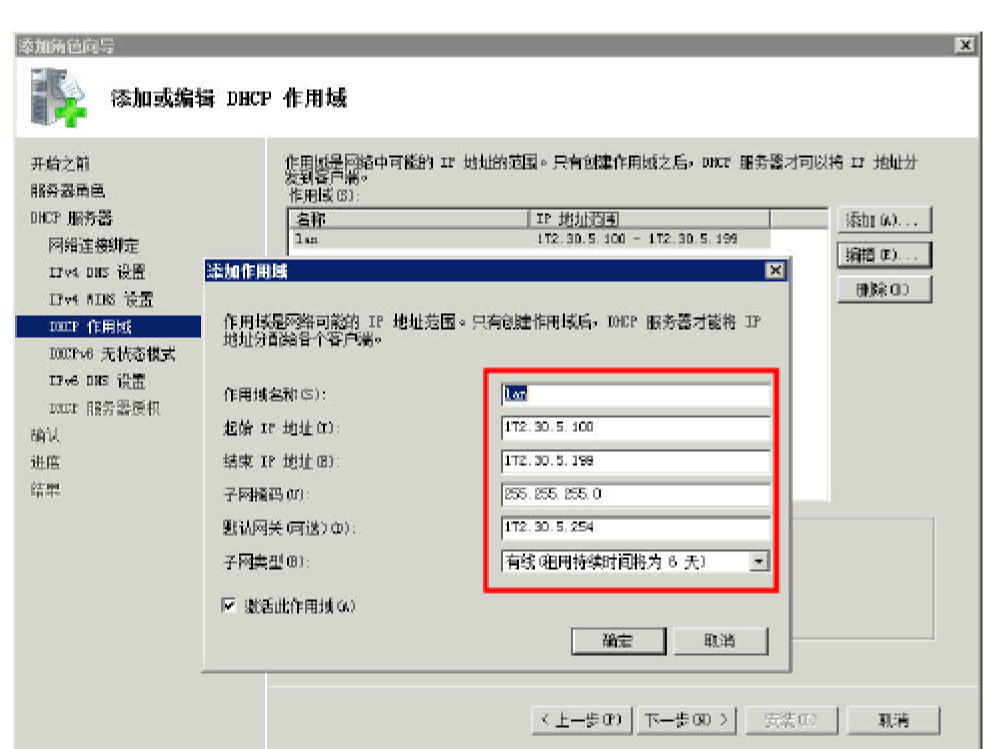


图 15-6　选择绑定地址

03 在“添加或编辑 DHCP 作用域”对话框中，为当前 DHCP 服务器添加作用域，作用域的地址范围是 172.30.5.100 ~ 172.30.5.199，如图 15-7 所示。

04 在“配置 DHCPv6 无状态模式”对话框中，选中“对此服务器禁用 DHCPv6 无状态模式”单选按钮，如图 15-8 所示。



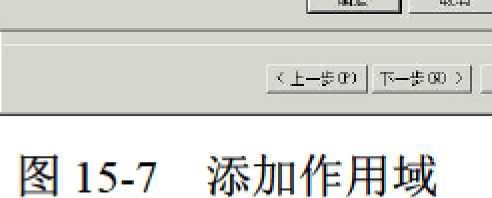


图 15-7　添加作用域

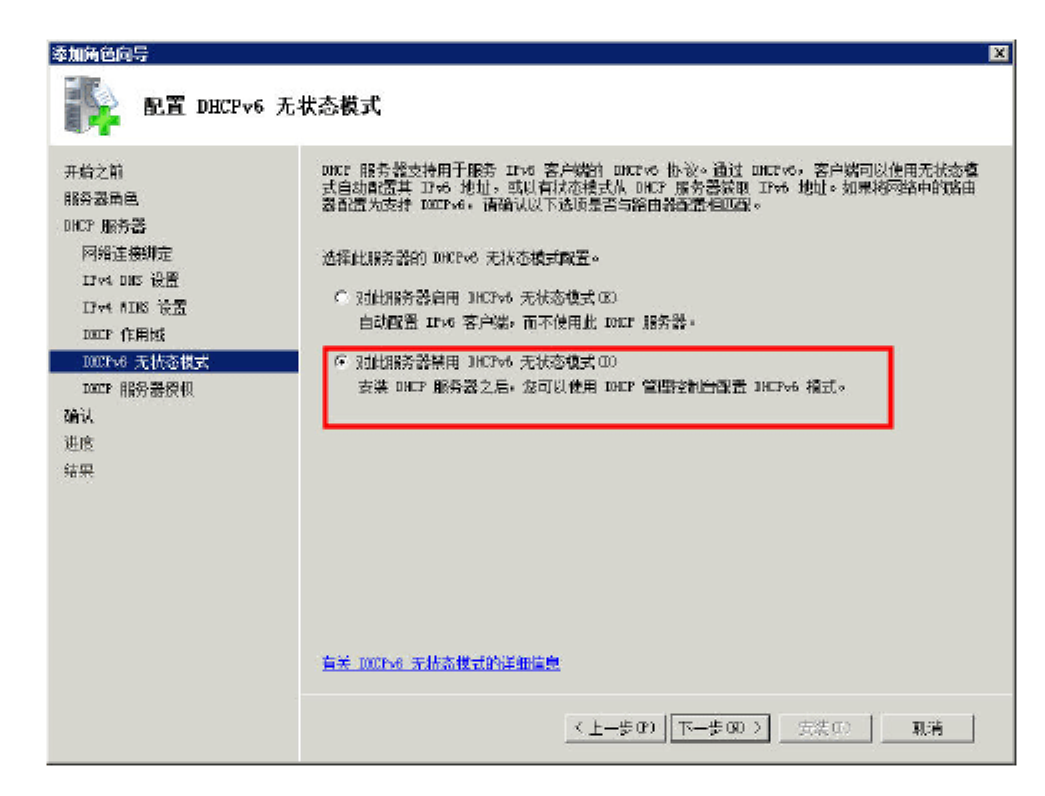


图 15-8　禁用 DHCPv6 无状态模式

05 安装 DHCP 服务器完成之后，在“服务器管理器”控制台中，定位到“DHCP 服务器”，删除其他的作用域（只保留图 15-7 创建的作用域），然后打开该作用域的“属性”对话框（如图 15-9 所示），在“高级”选项卡中，选中“两者”单选按钮，如图 15-10 所示。

06 最后在“IPv4 属性”对话框的“高级”选项卡中，为 DHCP 服务器绑定 172.30.5.15 的服务器地址，如图 15-11 所示。

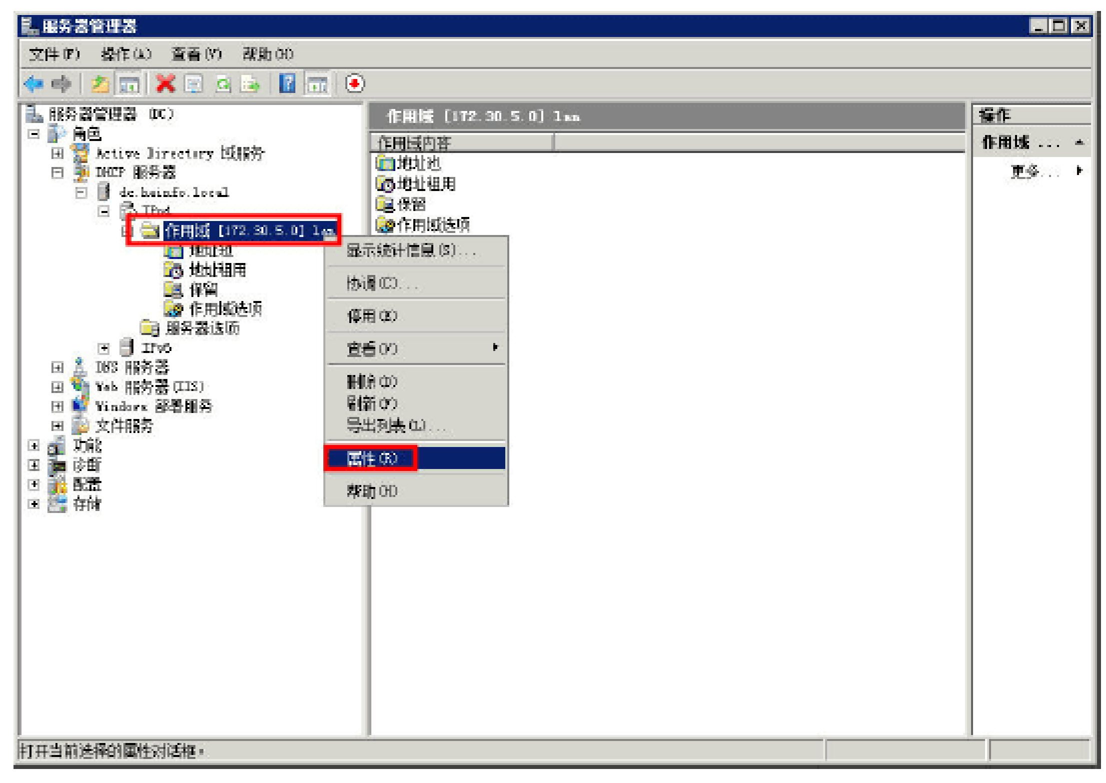



图 15-9　作用域属性

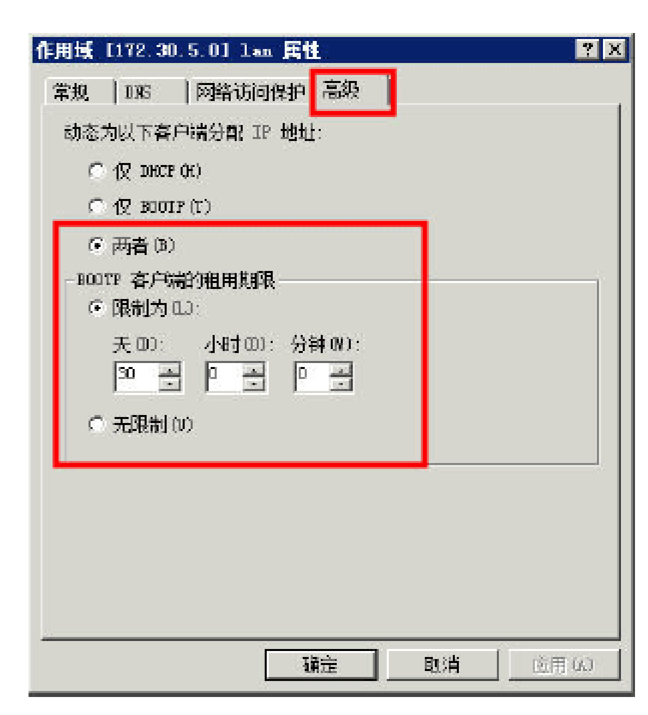
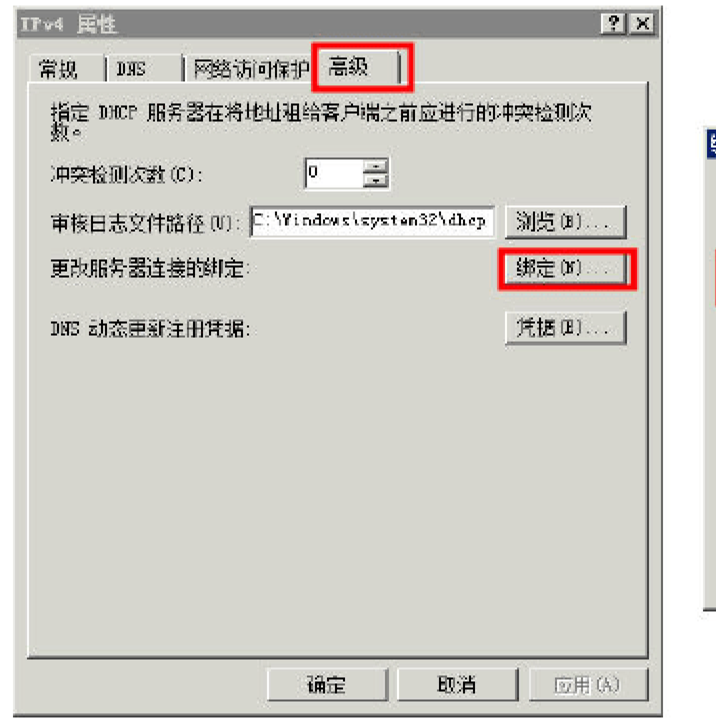


图 15-10　启用 DHCP 与 BOOTP



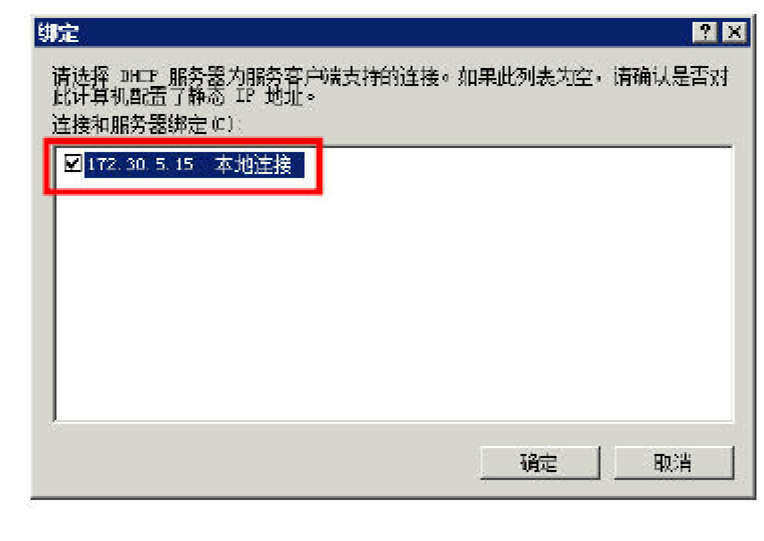


图 15-11　绑定 DHCP 服务器的地址

15.4　启动 Windows 部署服务

在“服务器管理器”控制台中（如果原来“服务器管理器”已经打开，请关闭并再次进入），定位到“角色→Windows 部署服务”，开始启动 Windows 部署服务。

下面介绍 Windows 部署服务的配置过程与步骤。

01 用鼠标右键单击“dc.heinfo.local”，从快捷菜单中选择“配置服务器”命令，如图 15-12 所示，启动“Windows 部署服务配置向导”。

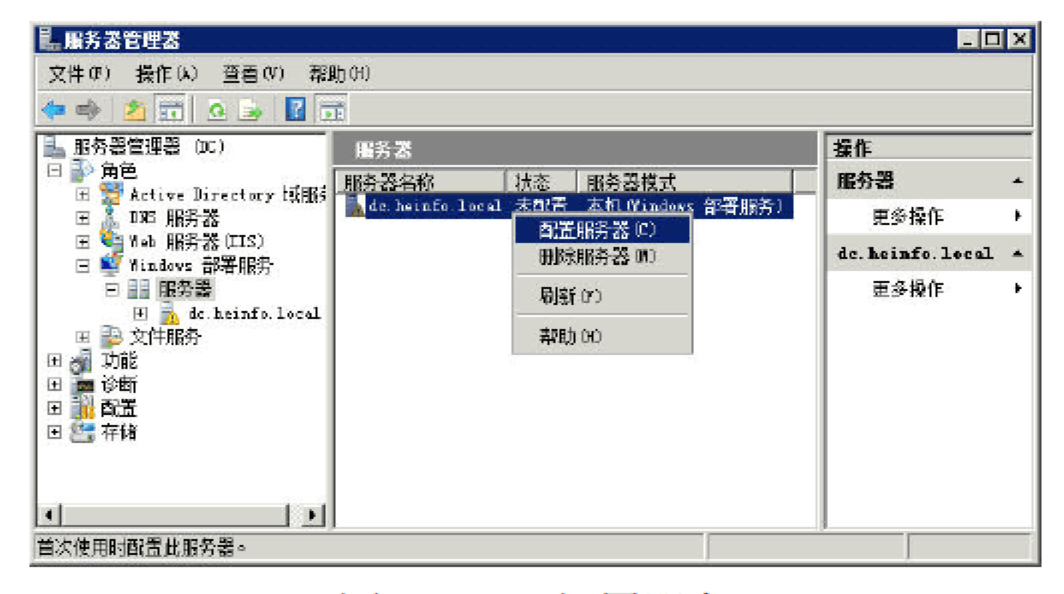


图 15-12　部署服务

02 在“欢迎页面”对话框列出了 Windows 部署服务所需要的条件，如图 15-13 所示。

03 在“远程安装文件夹的位置”对话框中，选择一个可用空间最大的 NTFS 分区，作为 Windows 部署服务保存操作系统映像的位置，如图 15-14 所示。

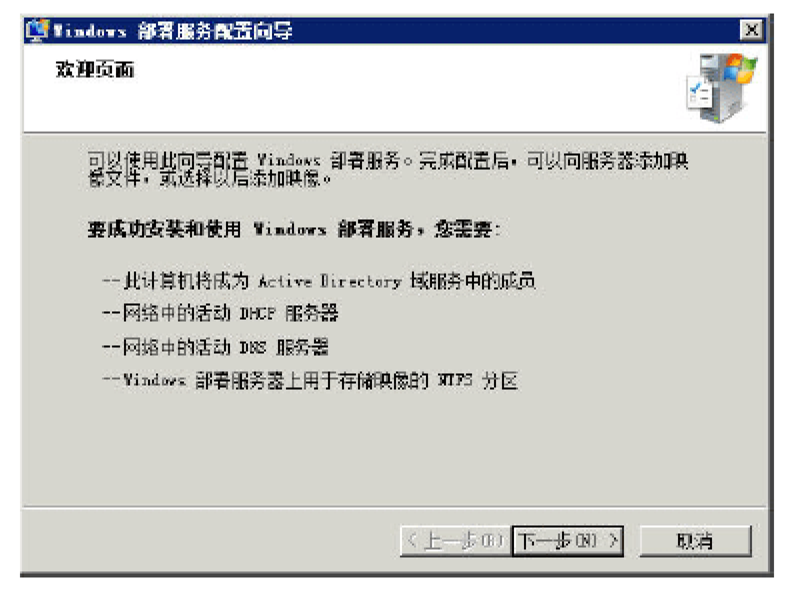


图 15-13　配置向导

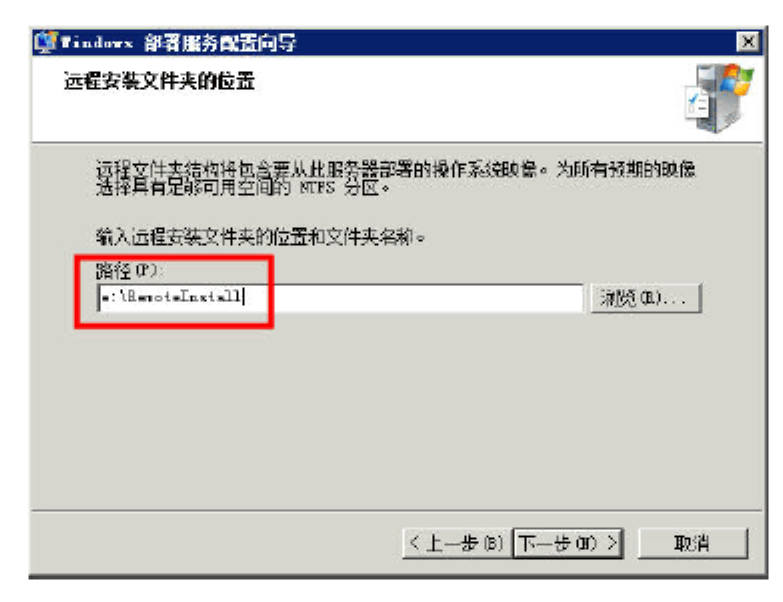


图 15-14　选择位置

04 在“DHCP 选项 60”对话框中，配置 DHCP 服务器。如果网络中的 DHCP 服务器与 Windows 部署服务在同一台计算机上，须选中“不侦听端口 67”和“将 DHCP 选项标记#60 配置为‘PXEClient’”复选框，如图 15-15 所示。

05 在“PXE 服务器初始设置”对话框中，选中“响应所有（已知和未知）客户端计算机”单选按钮，如图 15-16 所示。

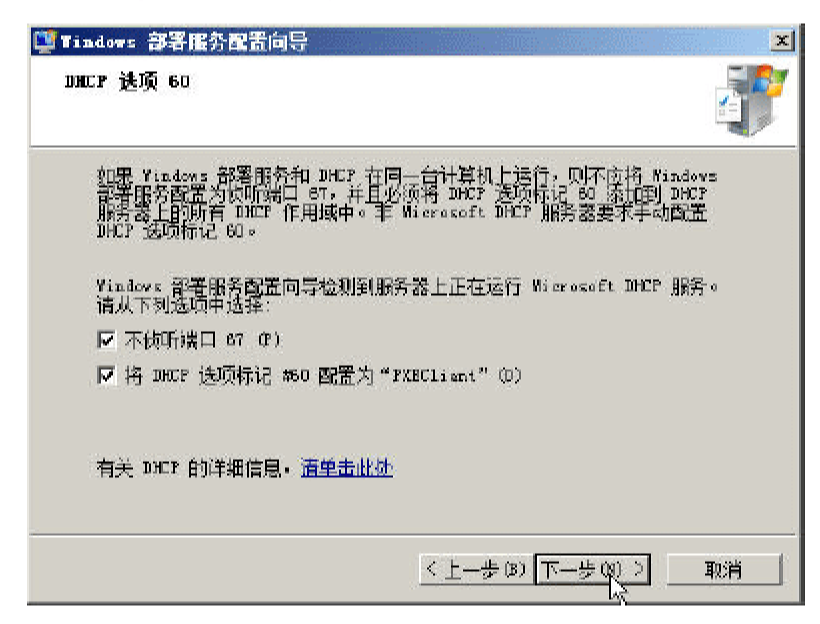


图 15-15　DHCP 选项

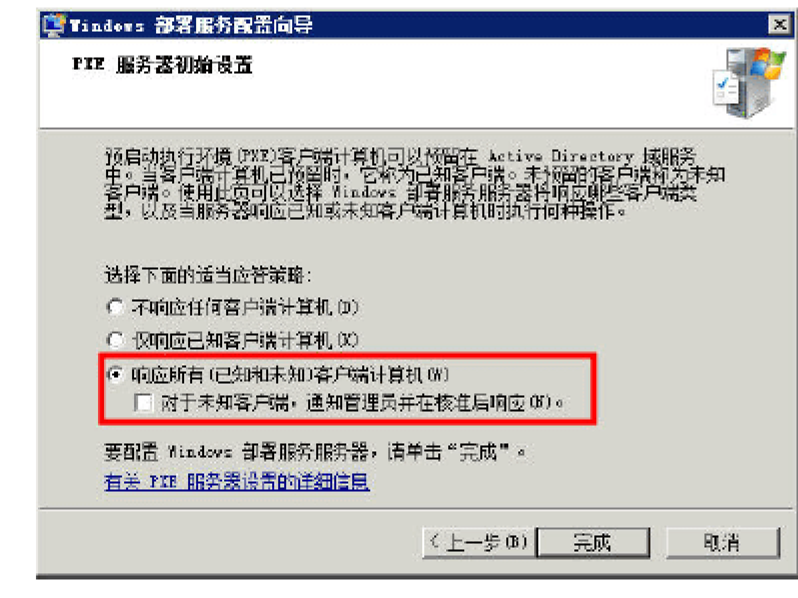


图 15-16　PXE 服务器初始设置

06 在“配置完成”对话框中，选中“立即在 Windows 部署服务器上添加映像”复选框，如图 15-17 所示。

07 在“Windows 映射文件位置”对话框中，选择将要添加的 Windows 操作系统的位置。在本例中，将 Windows 7（集成 SP1）的 32 位安装光盘放在光驱中，该光驱的盘符为 D。在本例中选择 D:\，如图 15-18 所示。

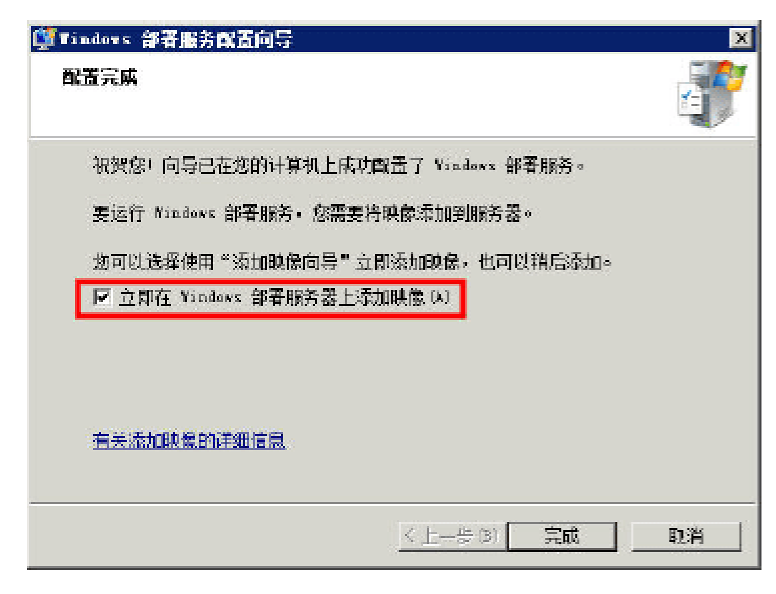


图 15-17　完成配置

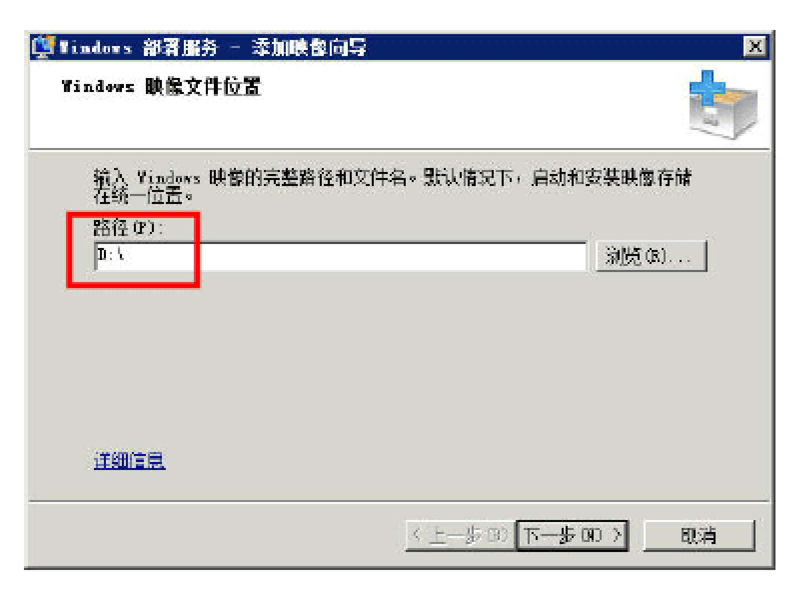


图 15-18　指定映像文件位置

08 在“映像组”对话框中，选中“创建新映像组”单选按钮，在此命名映像组名称为“Windows 7 SP1”，如图 15-19 所示。

09 在“复查设置”对话框中，显示了图 15-19 中要添加的映像数，分别为“启动映像数”与“安装映像数”，如图 15-20 所示。

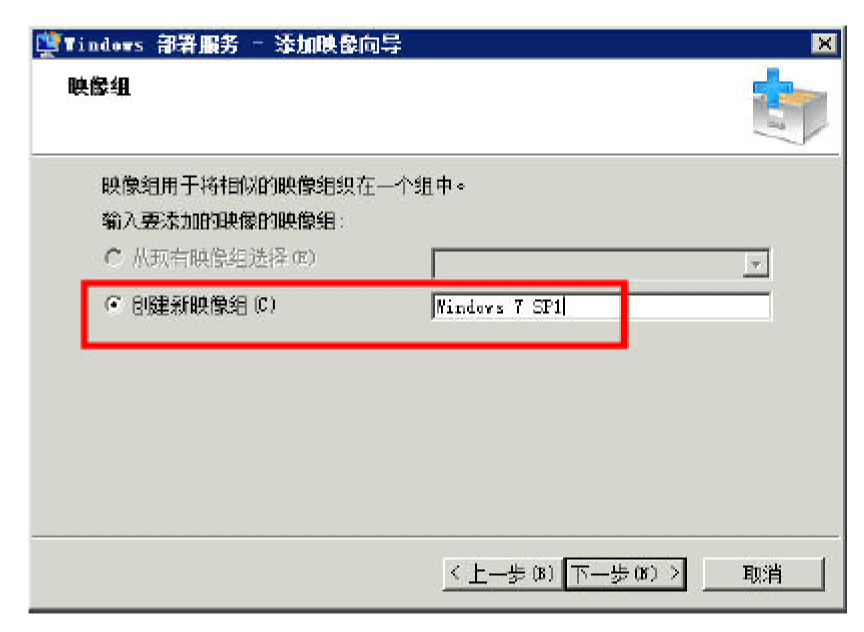


图 15-19　创建新映像组

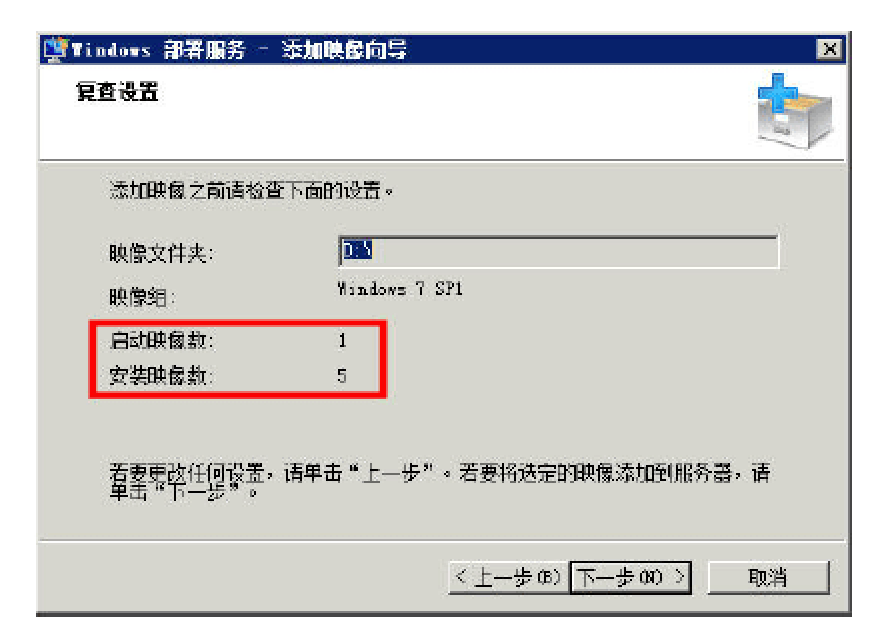


图 15-20　复查设置

说 明

“启动映像”是用来启动计算机的操作系统映像，“安装映像”是用来安装计算机的操作系统。从 Windows Vista 开始，启动映像与安装映像分开。使用“高版本”的启动映像启动计算机，可以安装“低版本”的操作系统，但低版本的启动映像启动计算机，将不能安装“高版本”的操作系统。例如，用 Windows 7 SP1 的启动映射启动计算机，可以用来安装 Windows Vista、Windows Server 2008、Windows Server 2008 R2、Windows 7、Windows 7 集成 SP1 包，但如果用 Windows Vista 的启动映像启动计算机，则不能安装 Windows 7、Windows Server 2008 R2 操作系统映像。

10 在“任务进度”对话框中，当操作系统的启动映像与安装映像添加到 Windows 部署服务器之后，显示“操作完成”，单击“完成”按钮，如图 15-21 所示。

11 返回到“服务器管理器”控制台，可以看到已经添加了 5 个 Windows 7 的安装镜像，分别是 Windows 7 的家庭基础版、家庭高级版、专业版、旗舰版、入门版，如图 15-22 所示。

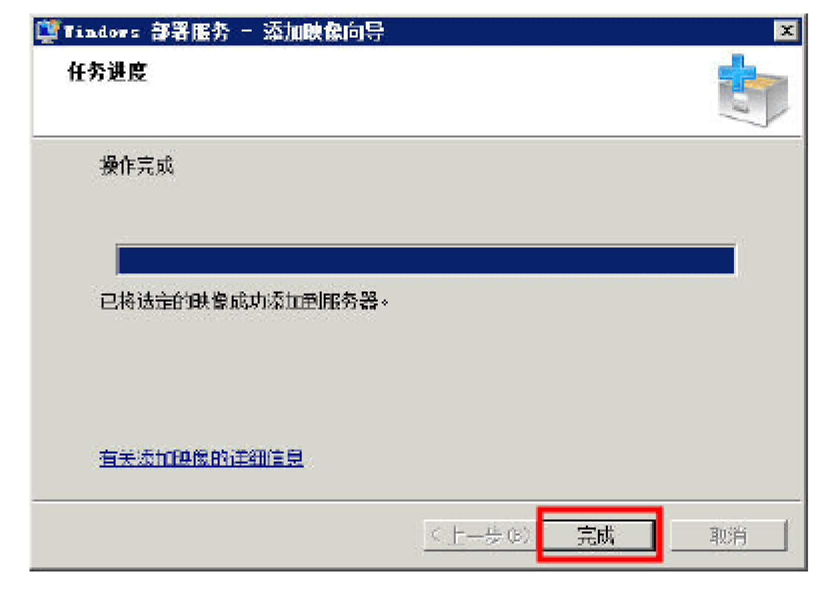


图 15-21　操作完成



图 15-22　Windows 7 安装映像

15.5　添加其他操作系统的安装镜像

前文介绍过，使用 Windows 部署服务，可以为网络中的计算机部署 Windows Vista、Windows 7、

Windows Server 2008、Windows Server 2008 R2 多个操作系统。如果要部署多个产品（例如 32 位与 64 位）、多个版本（例如 Windows 7、Windows 7 集成 SP1、Windows Server 2008 等），推荐为每个不同的产品与版本，创建单独的“映像组”，并在映像组中，添加对应的操作系统的安装映像。等以后有新的版本了，或者该版本的安装映像不再使用，可以直接通过删除该映像组的方式，从服务器中删除该安装映像以释放磁盘空间。下面，以添加 Windows 7 SP1 的 64 位安装映像为例，介绍创建映像组、向映像组中添加安装映像的方法，步骤如下。

01 在“服务器管理器”控制台中，定位到“服务器管理器→角色→Windows 部署服务→服务器→（服务器计算机名）→安装映像”，在右侧空白窗格中用鼠标右击，在弹出的快捷菜单中选择“添加映像组”命令，如图 15-23 所示。

02 在“添加映像组”对话框中，输入要创建的组名，在本例中为“Windows 7 SP1 X64”，如图 15-24 所示。

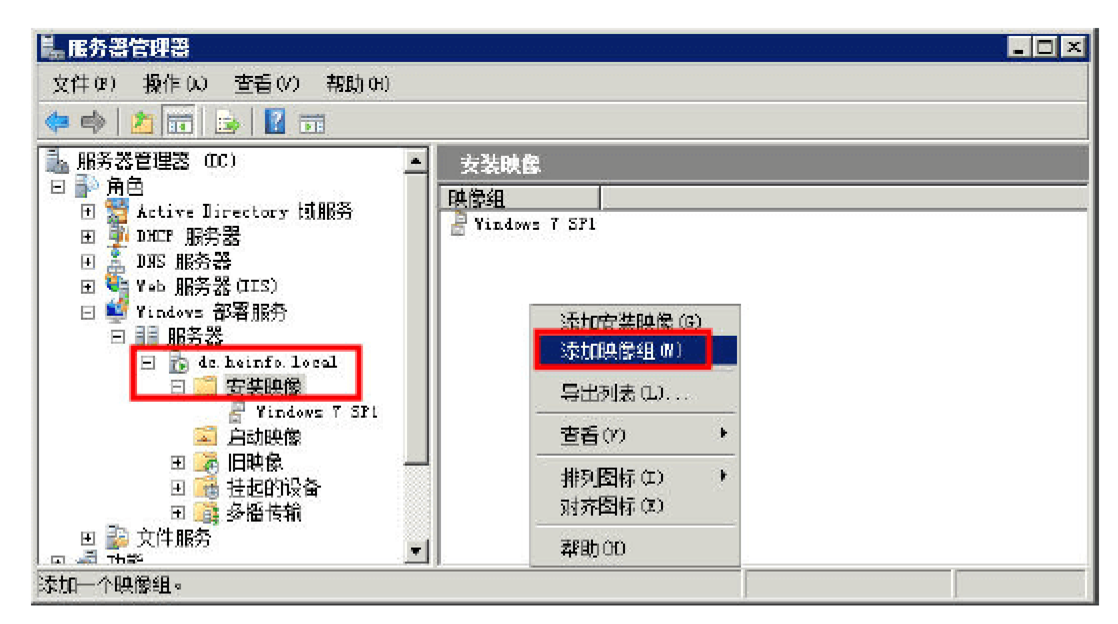


图 15-23　添加映像组



图 15-24　创建新映像组

03 然后定位到新创建的映像组，在右侧的空白窗格中用鼠标右击，在弹出的快捷菜单中选择“添加安装映像”命令，如图 15-25 所示。

04 然后在光驱中，换上 Windows 7 集成 SP1 的 64 位版本，在“映像文件”对话框中，浏览选择 Windows 7 安装光盘根目录中\sources\install.win 文件，如图 15-26 所示。

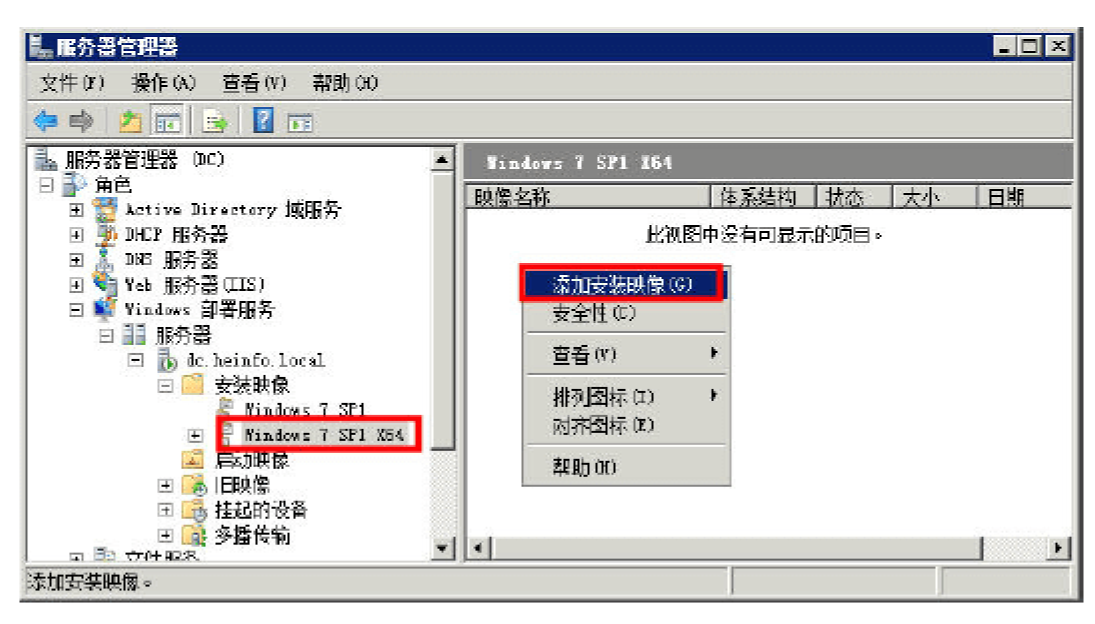


图 15-25　添加安装映像

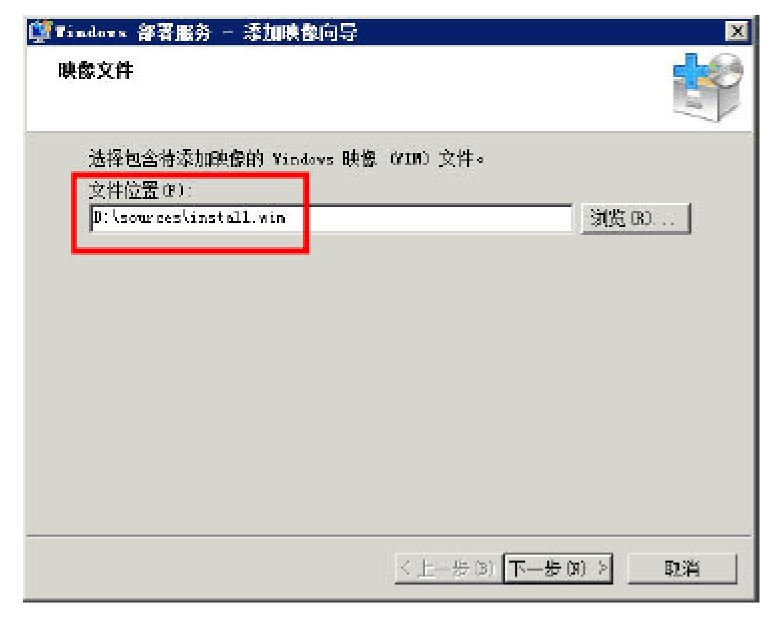


图 15-26　选择安装映像



说 明

在 Windows Vista 及其以后的操作系统安装光盘的 sources 目录中，有 2 个映像文件，其中名为 install.win 的是安装映像，名为 boot.win 是启动映像。

05 在“可用映像列表”对话框中，显示了可用的映像列表及描述信息，如果采用默认的名称与描述，须选中“使用每个选定映像的默认名称和说明”复选框；如果想修改默认名称及说明，须取消选中“使用每个选定映像的默认名称和说明”复选框，如图 15-27 所示。

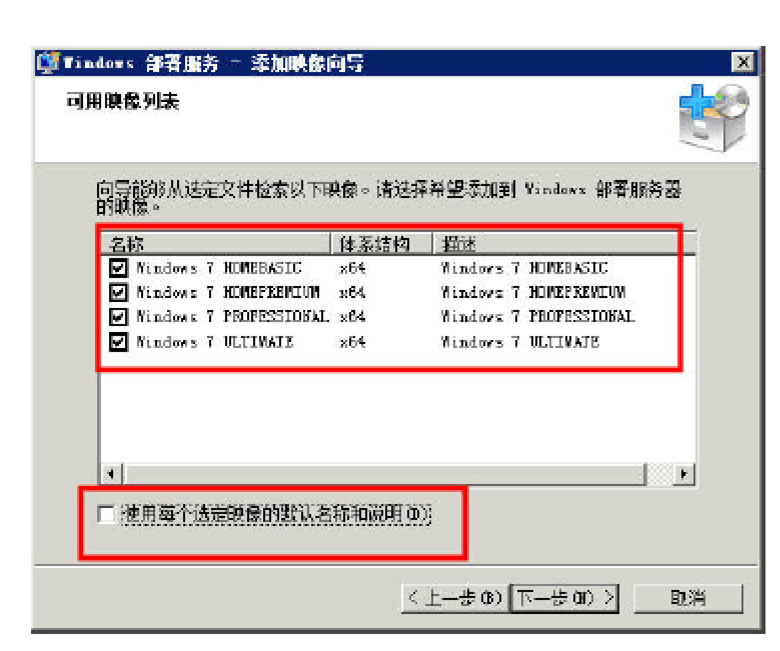


图 15-27　可用映像列表

06 如果在图 15-27 中取消选中“使用每个选定映像的默认名称和说明”复选框，则会弹出“映像元数据”对话框，并依次显示每个映像的名称及说明，可以根据需要修改进行修改，如图 15-28 与图 15-29 所示。

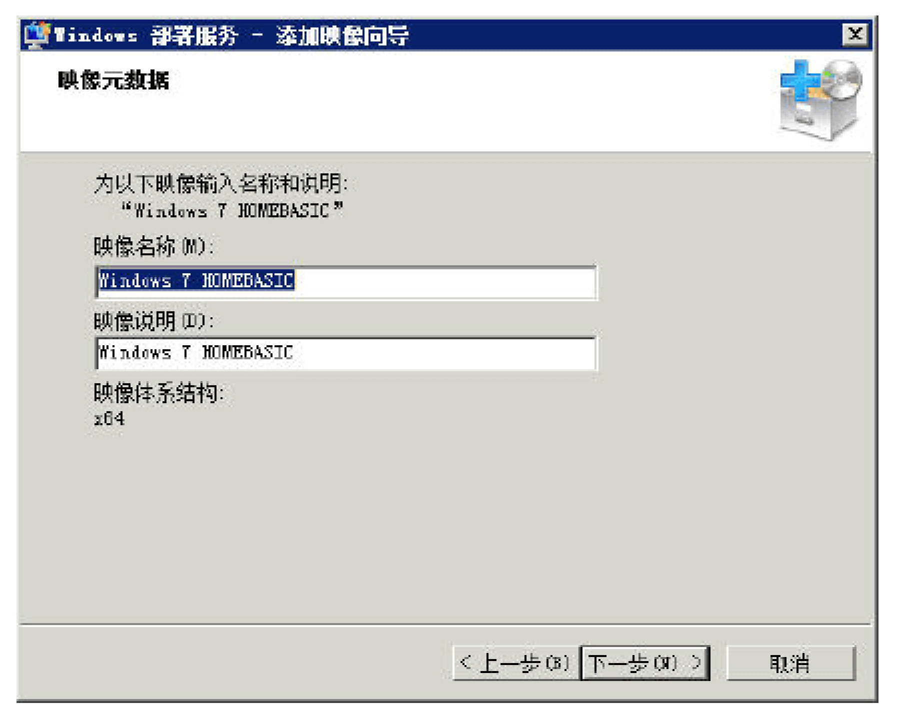


图 15-28　修改前

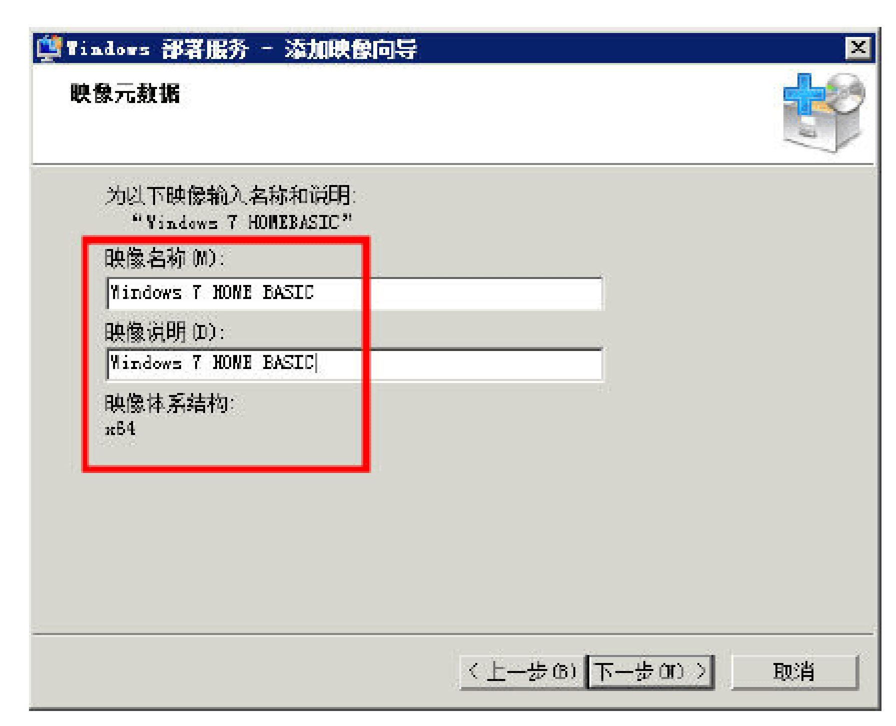


图 15-29　修改后

07 在“摘要”对话框中，显示要添加的映像，如图 15-30 所示。

08 添加映像完成后，单击“完成”按钮，如图 15-31 所示。

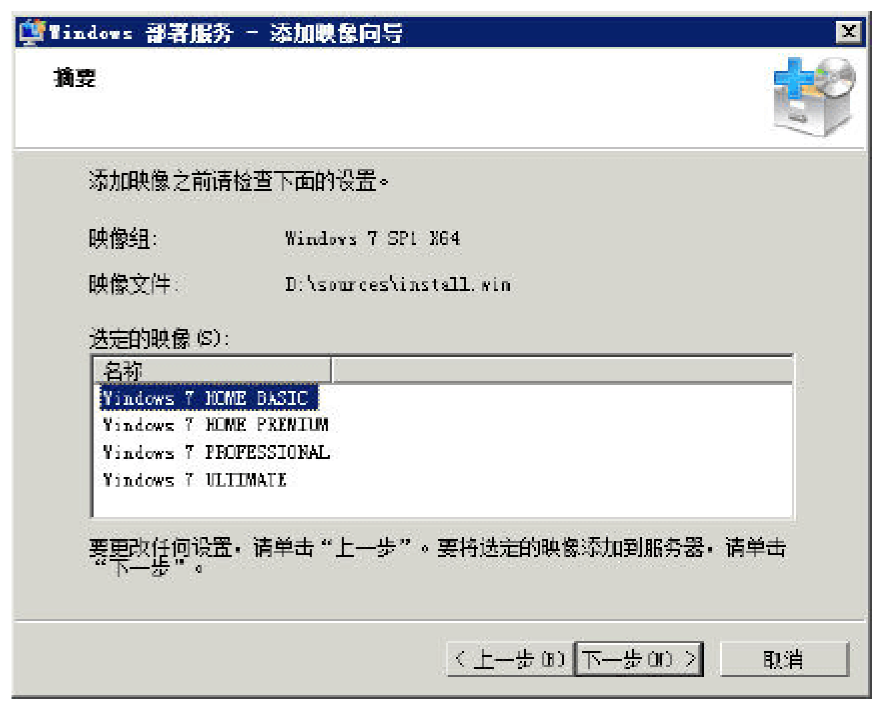


图 15-30　摘要

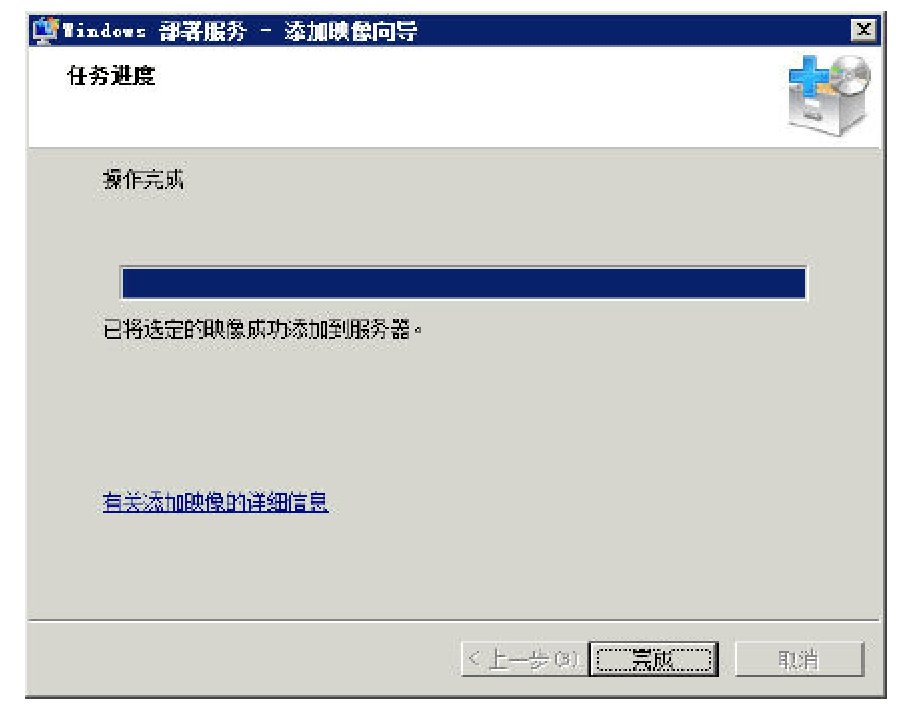


图 15-31　添加映像完成

如果你要添加其他操作系统的映像，可参照前面的步骤，创建映像组并添加映像，这些不再一一介绍。

15.6 添加启动映像

在添加安装映像之后，需要添加启动映像，需要注意的是，并不是每次添加安装映像，都要添加启动映像。如果已经有“同版本”的启动映像，则不用添加。Windows 启动映像与安装映像的关系是：

（1）Windows 7 SP1 与 Windows Server 2008 R2 SP1 的启动映像相同，是同一版本。目前该版本的启动映像，可以启动并安装包括 Windows 7 SP1、Windows Server 2008 SP1 及其以前的操作系统，例如 Windows Vista、Windows Server 2008、Windows Server 2008 SP2 等。

（2）Windows 启动映像也分 32 位与 64 位，32 位的启动映像可以安装 32 位与 64 位的操作系统；而 64 位的启动映像，只能安装 64 位的操作系统。如果 Windows 部署服务中，同时有 32 位与 64 位的启动映像，则在使用 Windows 部署服务的时候，会自动侦测客户端的类型，如果符合安装 64 位操作系统的要求，则会出现 32 位与 64 位启动映像的选项，让用户选择。如果不符合 64 位操作系统的要求，则会默认加载 32 位的启动映像。

（3）在添加更新版本的启动映像之后，可以删除以前版本的启动映像。

接下来，介绍添加启动映像的方法，以添加 64 位的 Windows 7 SP1 的启动镜像为例，步骤如下。

01 在“服务器管理器”控制台中，在“Windows 部署服务”中，定位到“启动映像”，在右侧空白窗格中右击，在弹出的快捷菜单中选择“添加启动映像”命令，如图 15-32 所示。

02 在“映像文件”对话框中，从 Windows 7 安装光盘中浏览选择名为 boot.win 的启动映像，如图 15-33 所示。

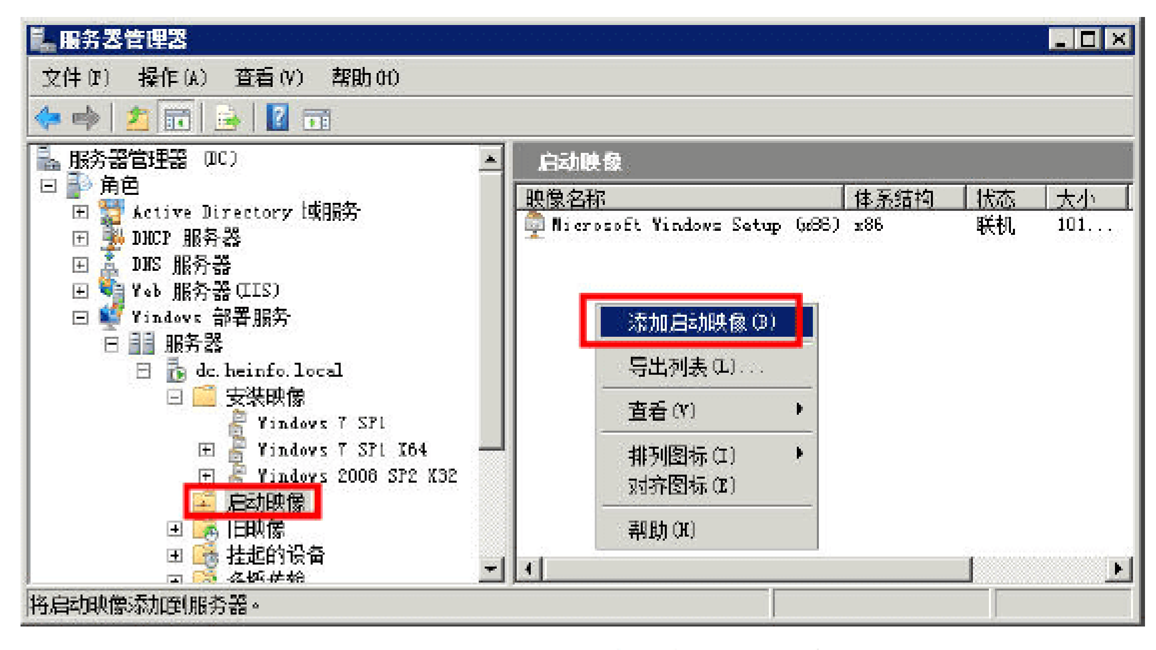



图 15-32 添加启动映像

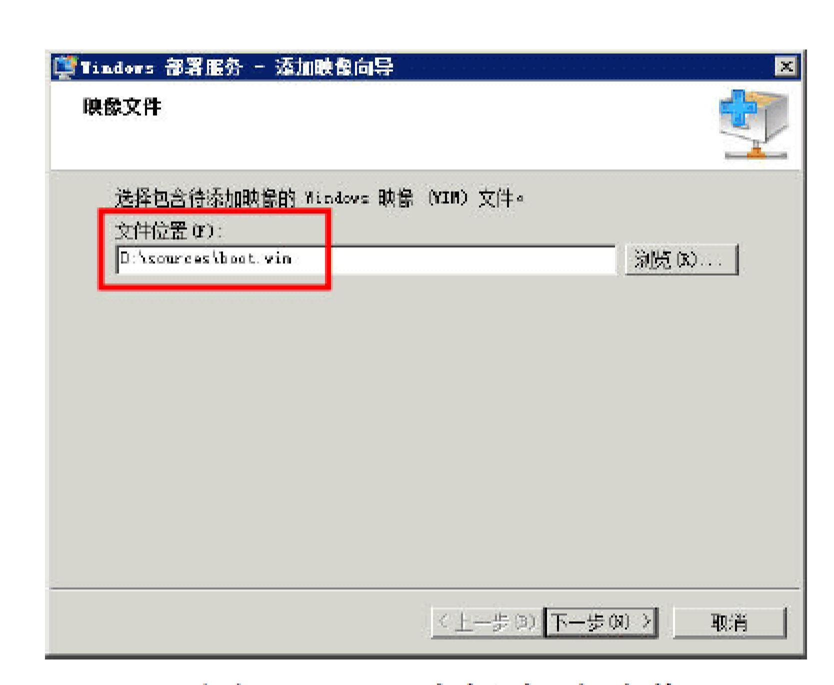


图 15-33 选择启动映像

03 在“映像元数据”对话框中，显示了添加的映像的名称与说明，也可以根据自己的需要或习惯进行定制，如图 15-34 所示。

04 在“摘要”对话框中，显示了要添加的映像的名称与位数（x64 表示 64 位），如图 15-35 所示。

05 添加完成之后，单击“完成”按钮，完成映像的添加，如图 15-36 所示。

06 添加启动映像之后，返回到“服务器管理器”控制台，定位到“Windows 部署服务”，在“启动映像”页，显示了添加的映像，如图 15-37 所示。

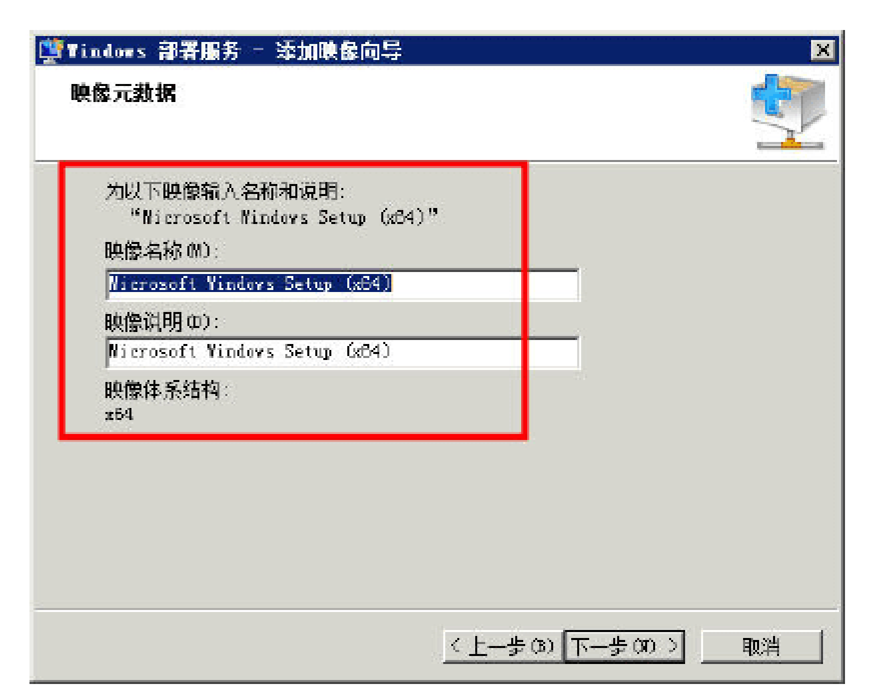


图 15-34　启动映像名称

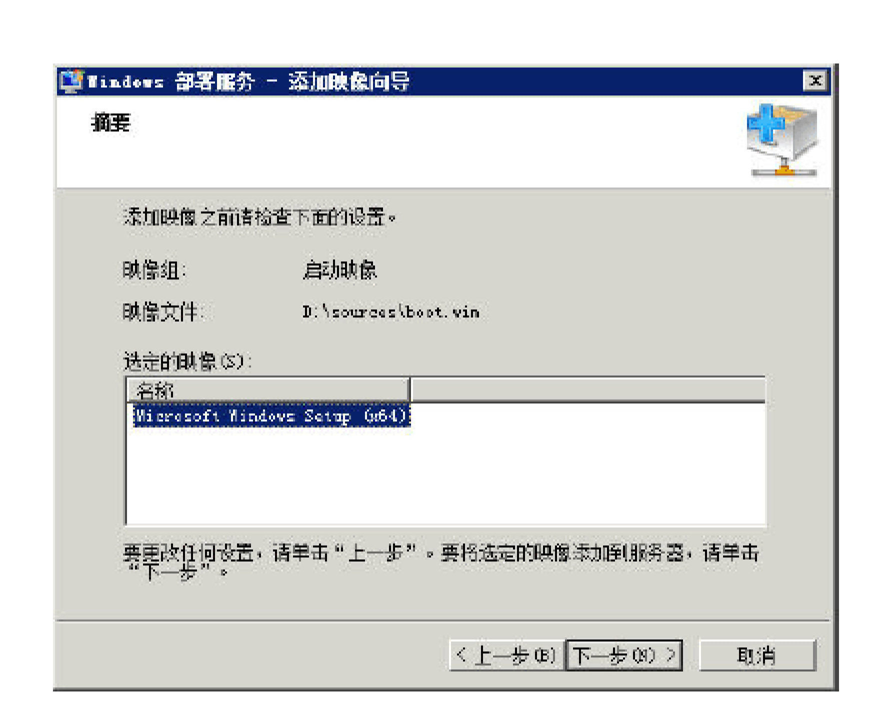


图 15-35　摘要

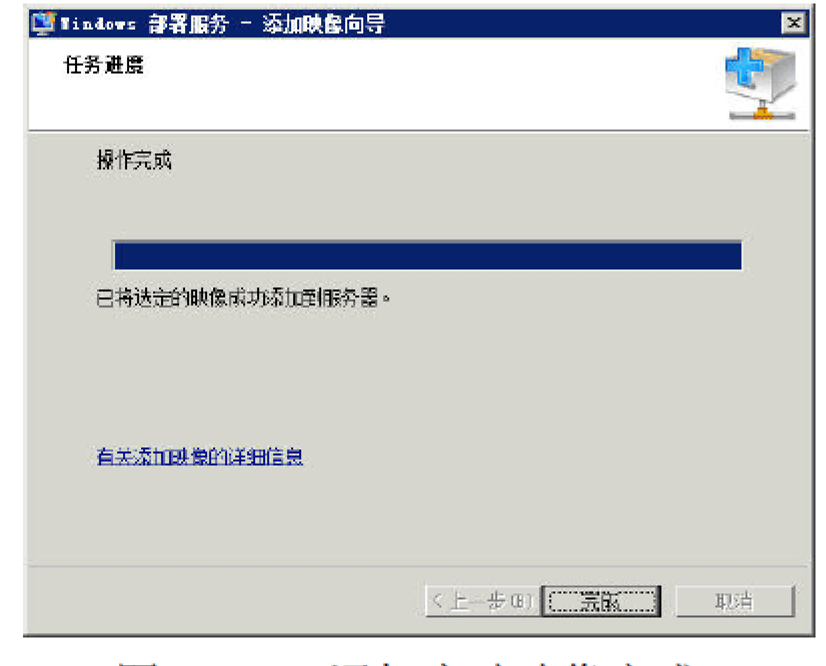


图 15-36　添加启动映像完成

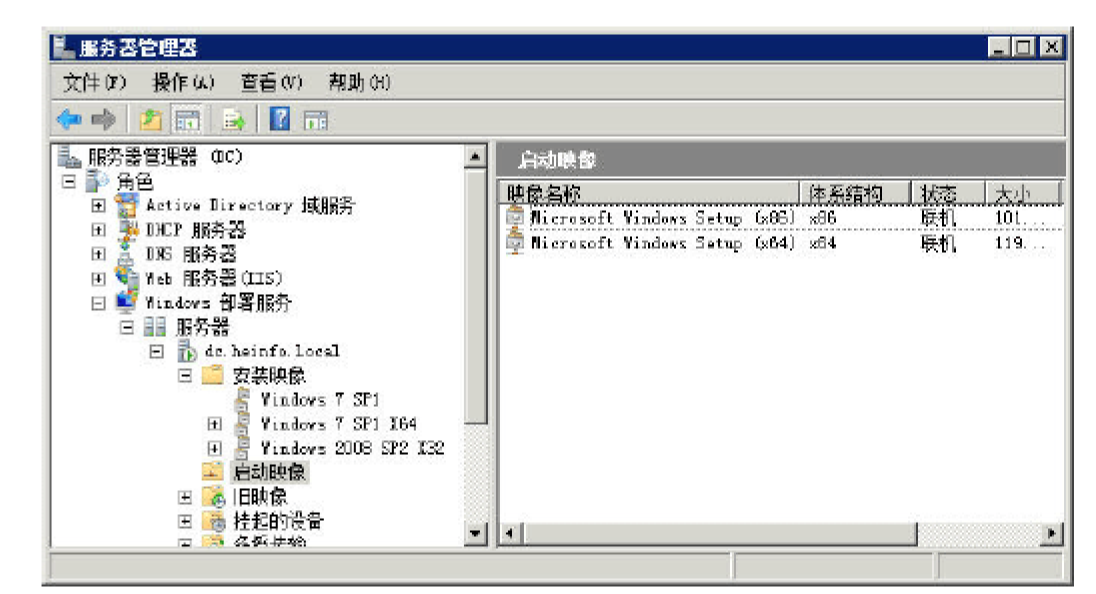


图 15-37　添加启动映像完成

如果要删除不再使用的映像，可以用鼠标右键单击映像，在弹出的快捷菜单中选择“删除”命令，并根据提示操作即可，如图 15-38 所示。

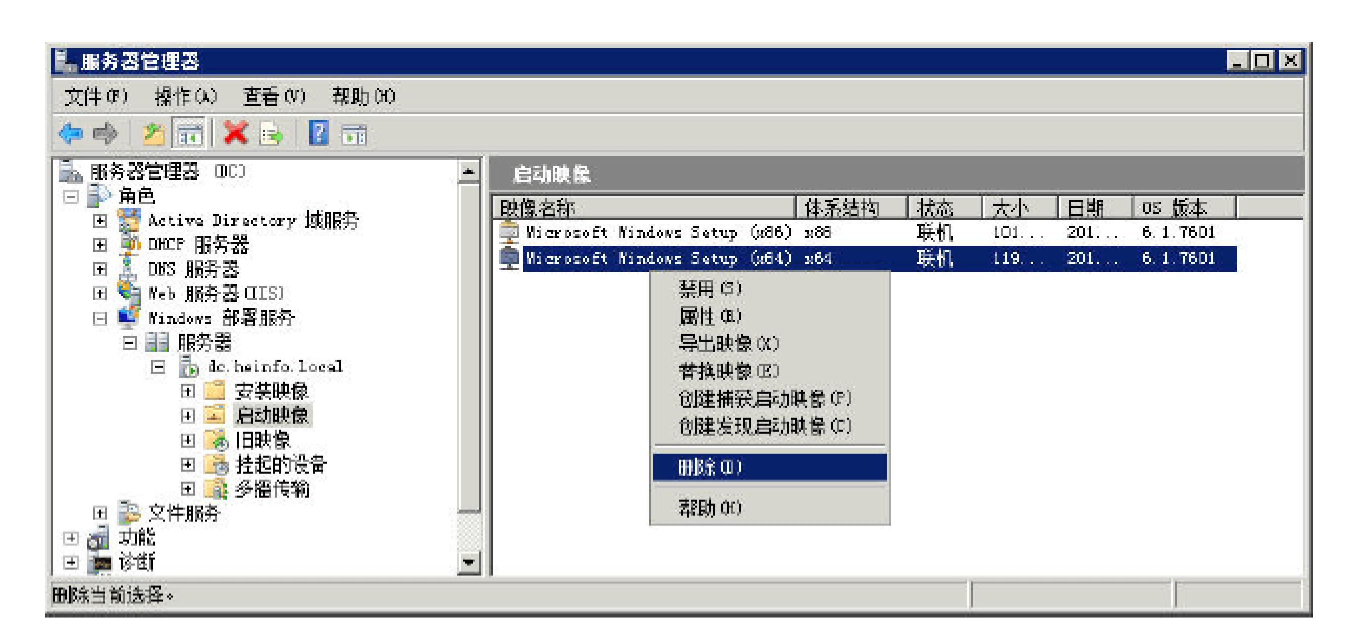


图 15-38　删除启动映像

15.7　配置 Windows 部署服务

在添加完安装映像与启动映像后，用鼠标右键单击服务器名“dc.heinfo.local”，从快捷菜单中选择“属性”选项（如图 15-39 所示），可以用来配置 Windows 部署服务器。

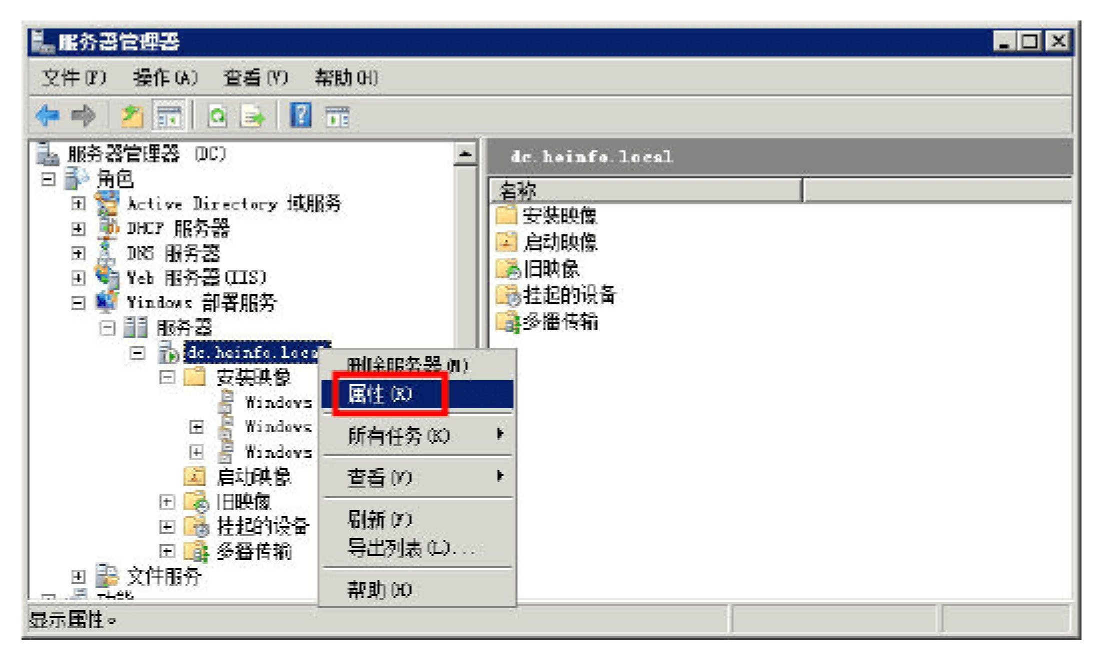


图 15-39　Windows 部署服务器属性

Windows 部署服务的主要设置如下。

01 在“DC 属性”对话框中，选择“PXE 响应设置”选项卡，选中“响应所有（已知和未知）客户端计算机”单选按钮，如图 15-40 所示。

02 选择“目录服务”选项卡，在“新建客户端命名策略”选项组中，设置客户端计算机的命名原则。在“客户端账户位置”选项组中，设置将使用 Windows 部署服务远程安装操作系统的计算机的保存位置，如图 15-41 所示。

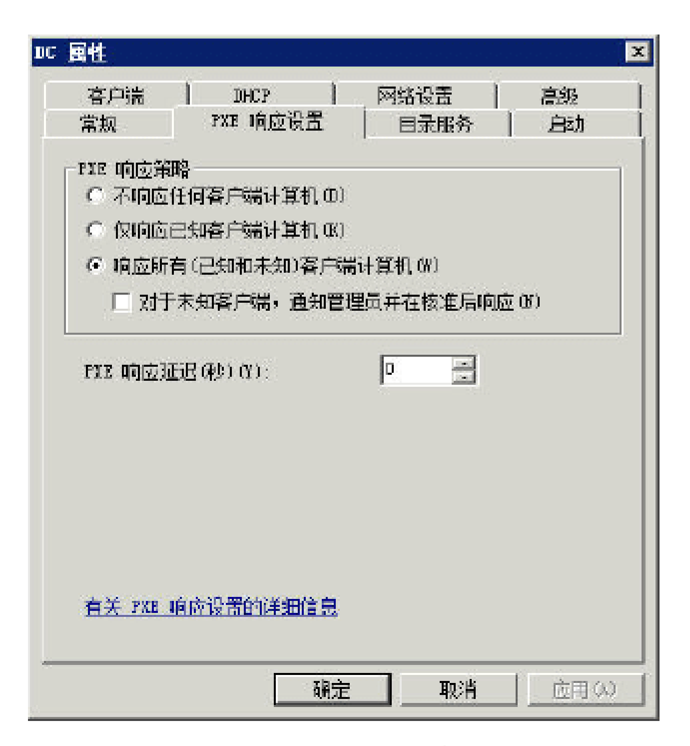


图 15-40　PXE 响应设置

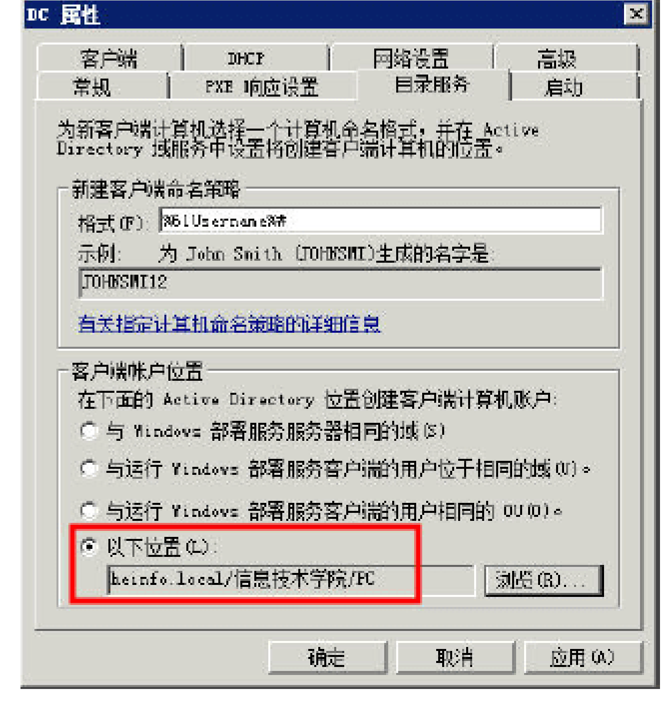
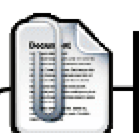


图 15-41　目录服务



说 明

在以前的 RIS 服务器中，使用 RIS 部署的计算机只能保存在 Active Directory 的“Computers”容器中，而在 Windows 部署服务中，可以将使用 Windows 部署服务安装操作系统的计算机统一保存在一个容器中。在本例中，将其保存在“heinfo.local/信息技术学院/PC”中。

03 在“启动”选项卡中，设置“默认启动程序”和“默认启动映像”，通常选择默认值即可，如图 15-42 所示。

04 在“高级”选项卡中，将选择 Windows 部署服务使用的 Active Directory 服务器和是否对 DHCP 服务器授权，须选中“在 DHCP 中授权 Windows 部署服务服务器”单选按钮，如图 15-43 所示。

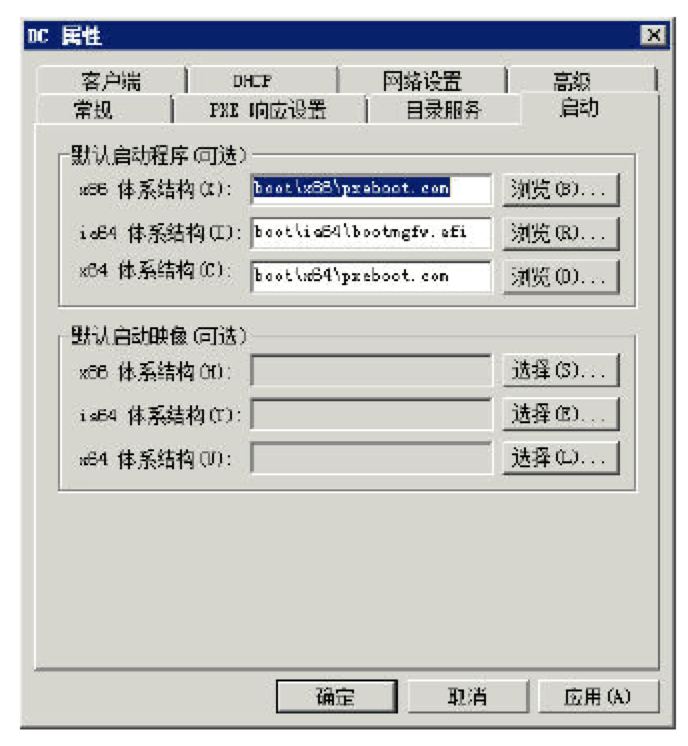


图 15-42　启动选项

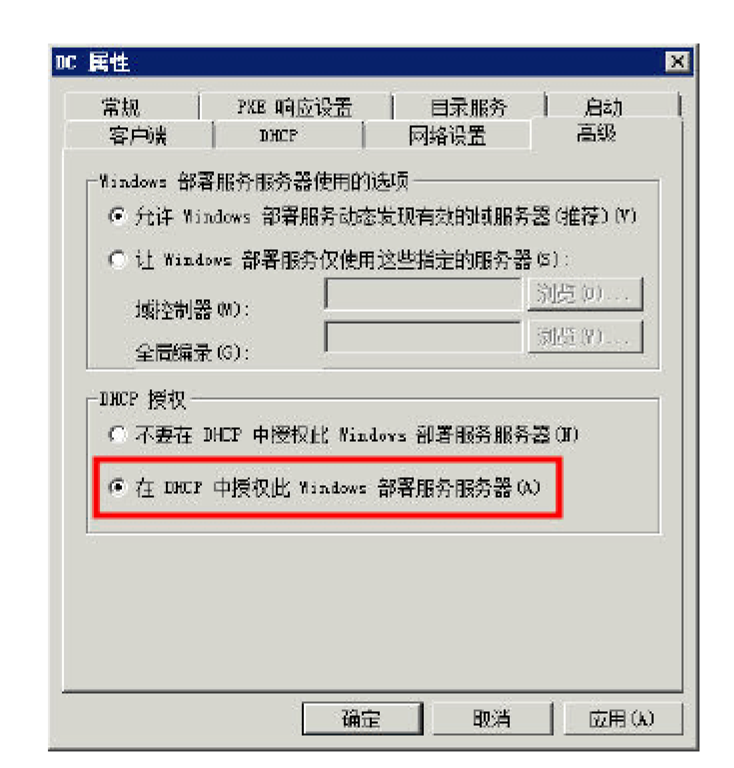


图 15-43　高级选项

05 在“DHCP”选项卡中，设置 DHCP 服务，如果当前服务器上有 DHCP 服务器，须选中“不侦听端口 67”和“将 DHCP 选项标记#60 配置为‘PXEClient’”复选框，如图 15-44 所示。

06 在“客户端”选项卡中，设置是否启用无人参与文件，如图 15-45 所示。

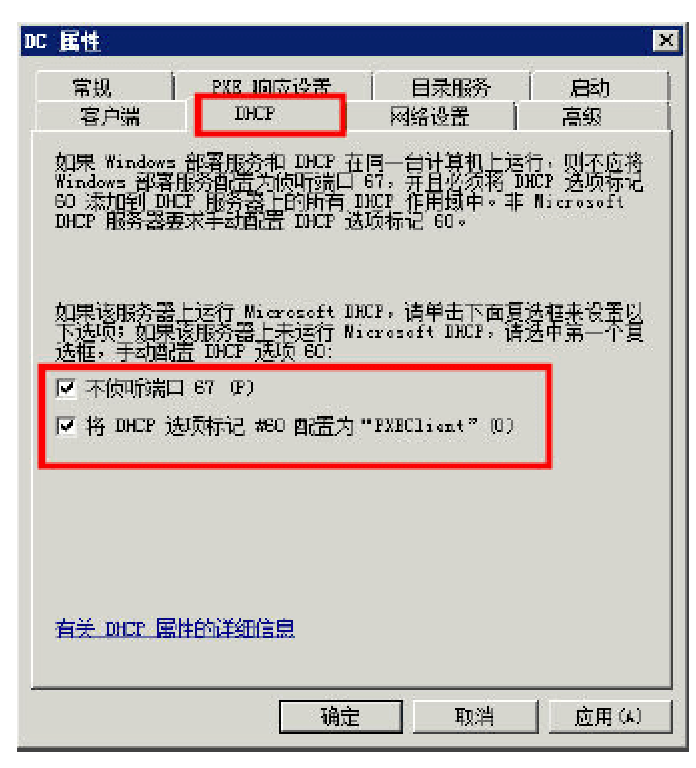


图 15-44　设置 DHCP

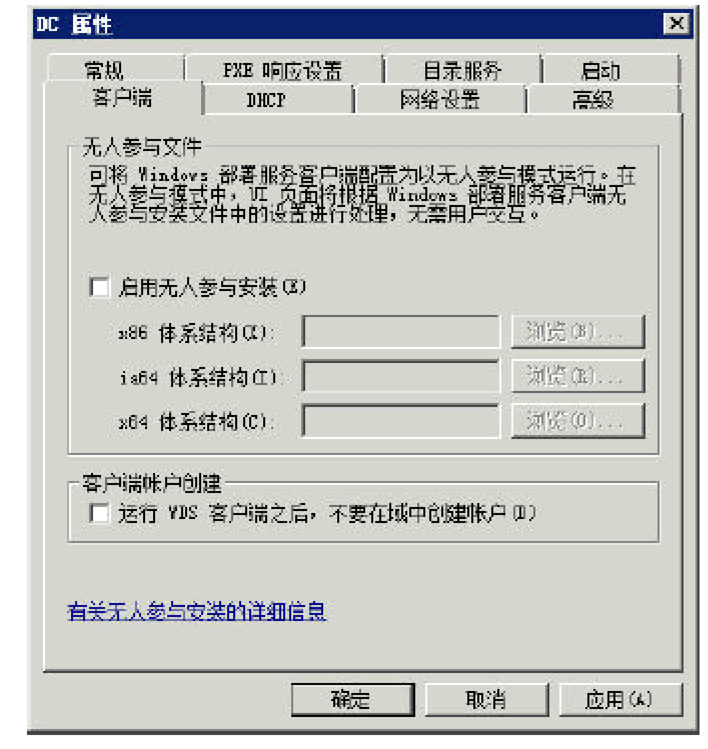


图 15-45　设置客户端

设置之后，单击“确定”按钮，完成 Windows 部署服务器的设置。

15.8　Windows 部署服务远程安装 Windows 7

接下来创建一个 Windows 7 的虚拟机，在虚拟机中，通过网络安装 Windows 7 操作系统，主要步骤如下。

01 创建 Windows 7 虚拟机后，启动虚拟机，当出现“Press F12 for network service boot”信息时，按 F12 键，如图 15-46 所示。

02 在“Windows 部署服务”对话框中，在“区域设置”下拉列表中选择“中文（简体，中国）”选项，在“键盘和输入方法”下拉列表中选择“中文（简体）-美式键盘”，如图 15-47 所示。

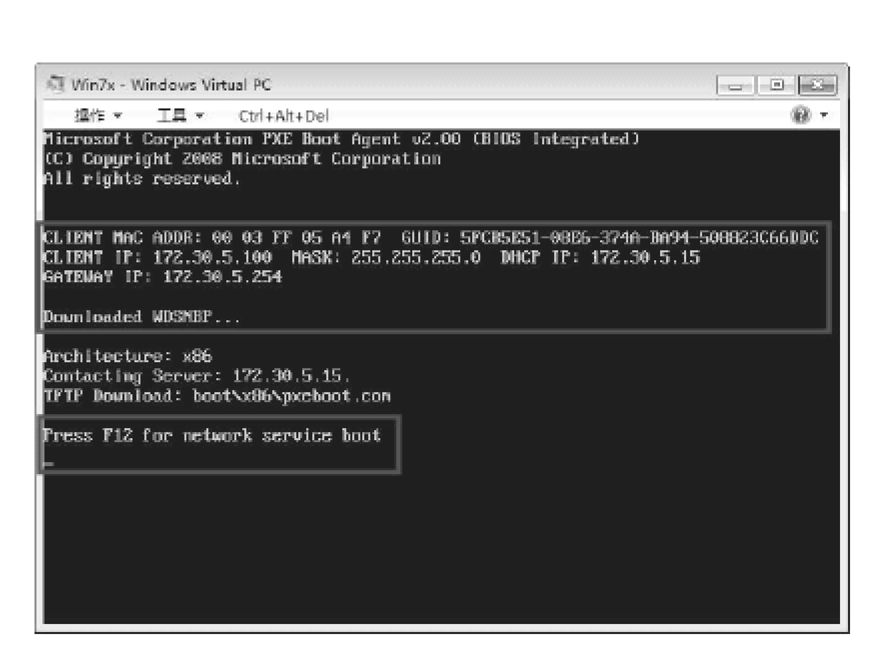
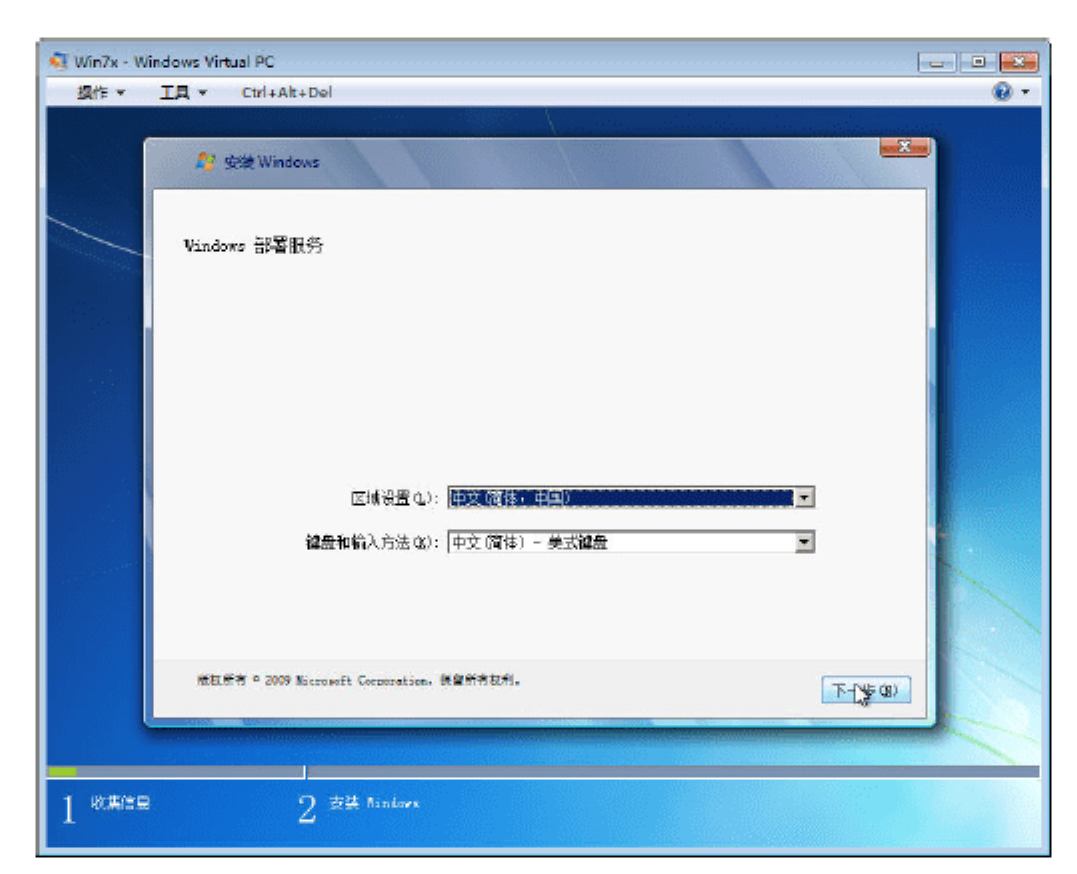
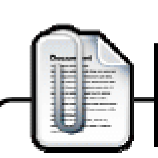



图 15-46　按 F12 从网络启动


图 15-47　选择语言

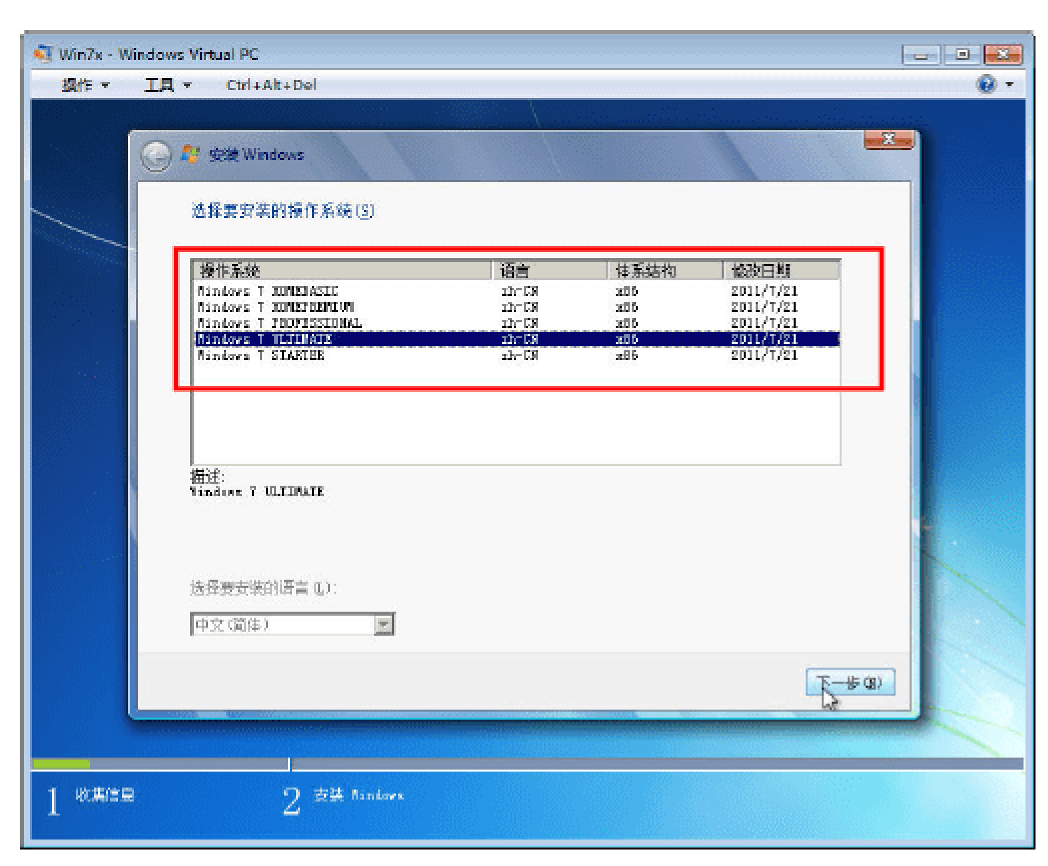
03 在“连接 dc.heinfo.local”对话框中，输入域用户名及密码，如图 15-48 所示。


说 明

要注意输入的用户名的格式，应为 heinfo.local\ws01 或 ws01@heinfo.local。

04 单击“下一步”按钮，显示“选择要安装的操作系统”对话框，选择需要的操作系统，如图 15-49 所示。


图 15-48　输入用户名和密码


图 15-49　选择要安装的操作系统

05 在“您想将 Windows 安装在何处”对话框中，根据需要对磁盘划分分区，并选择系统将要安装的分区，一般选择 C 盘分区，如图 15-50 所示。

06 设置完成后单击“下一步”按钮，显示“正在安装 Windows……”对话框，Windows 7 将开始安装，这一步大约需要 15~20min 的时间，如图 15-51 所示。

07 在“设置 Windows 7 旗舰版”对话框中，选择时区等设置，如图 15-52 所示。

08 在“输入用户名”文本框中，为 Windows 7 设置计算机名称，如图 15-53 所示。

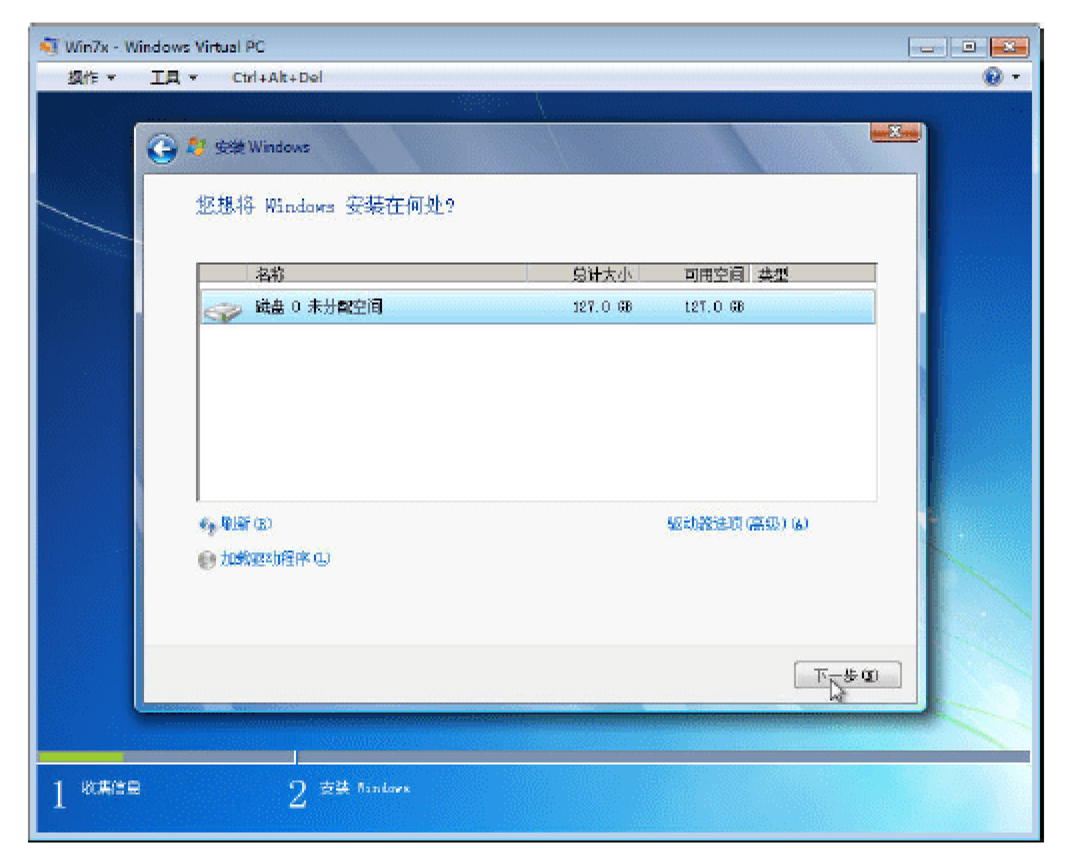


图 15-50　选择分区

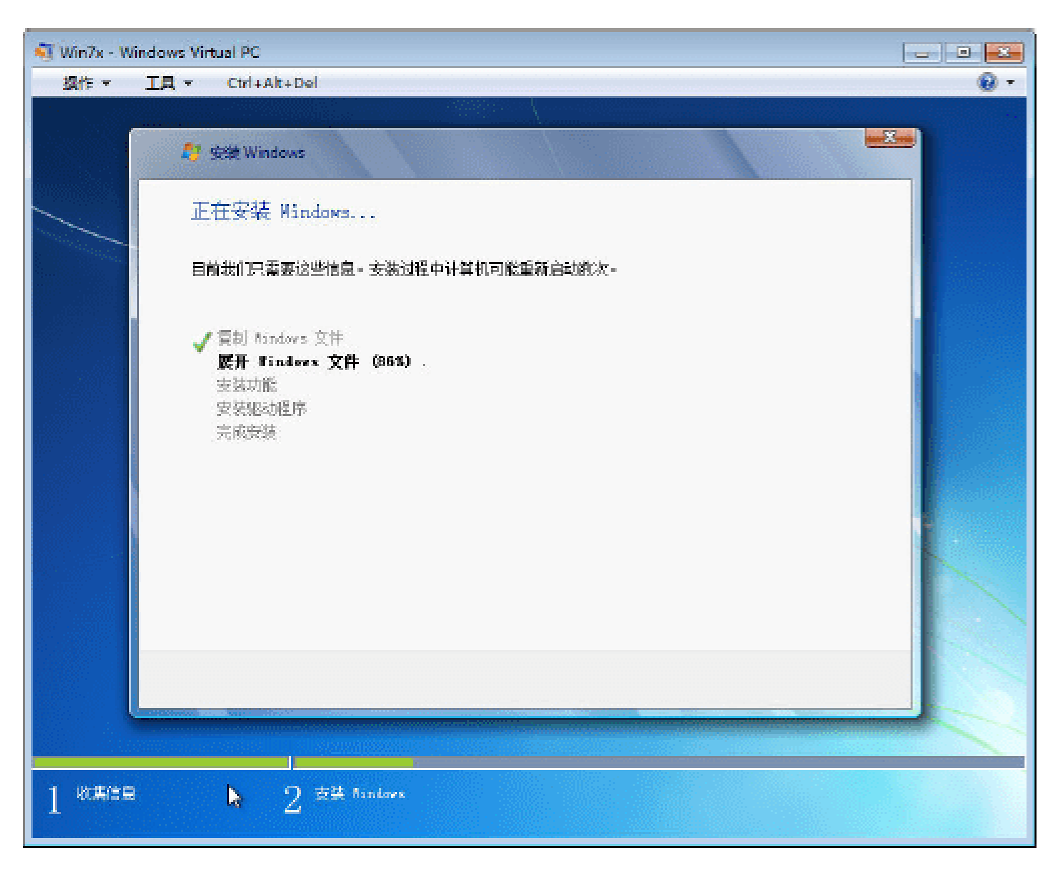


图 15-51　正式安装



图 15-52　设置 windows



图 15-53 设置计算机名称

09 在“输入您的 Windows 产品密钥”对话框中，输入 Windows 7 的安装序列号，或者单击“跳过”按钮，如图 15-54 所示。

10 在“请阅读许可条款”对话框中，选中“我接受许可条款”复选框，如图 15-55 所示。

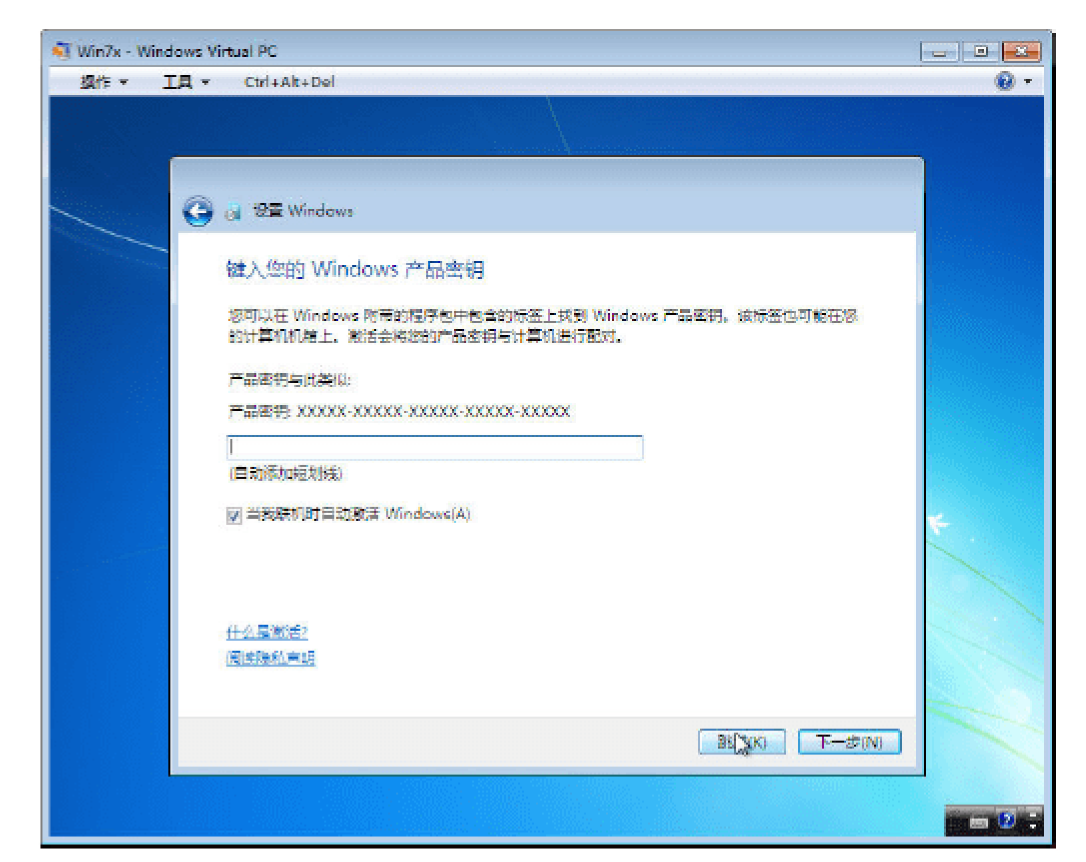


图 15-54　输入序列号



图 15-55　接受协议

11 在 Windows7 旗舰版登录界面中，输入域用户名与密码。在本例中，用户名为 ws01，如图 15-56 所示。

12 使用域用户名与密码登录之后，进入 Windows 7，安装完成，如图 15-57 所示。

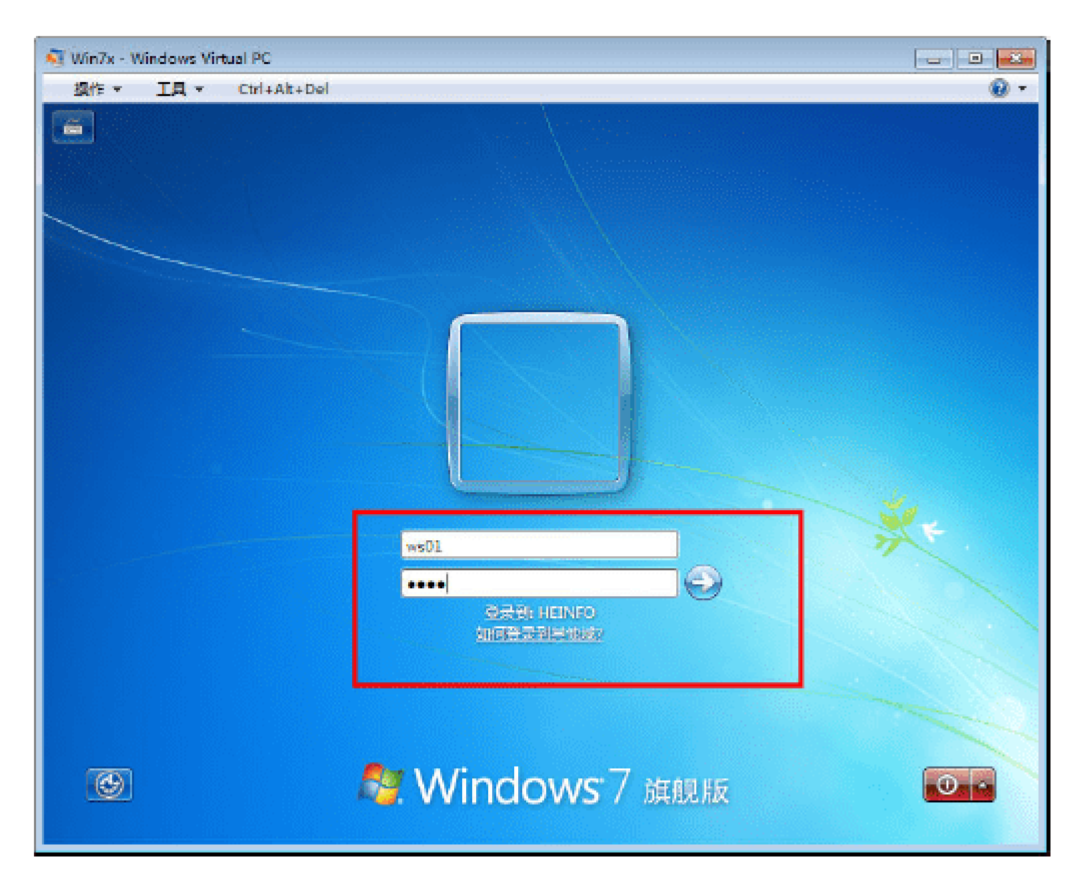


图 15-56　域用户登录

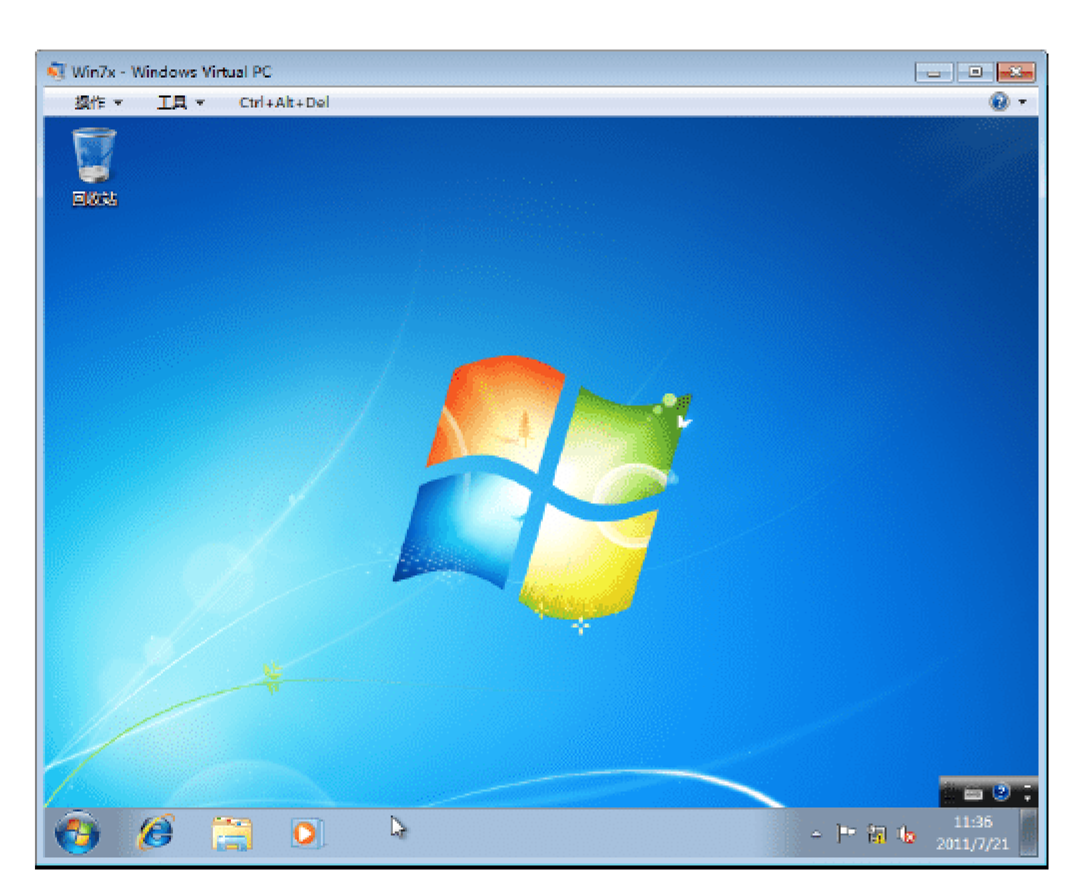


图 15-57　安装完成

15.9　出现 0x80070002 错误的解决方法

如果网络中原来存在 Windows 部署服务，并添加了新版本的安装映像（例如原来使用的是 Windows Server 2008，而现在添加了 Windows Server 2008 R2 的安装映像），在部署 Windows Server 2008 R2 的时候，将出现 0x80070002 的错误提示，如图 15-58 所示。

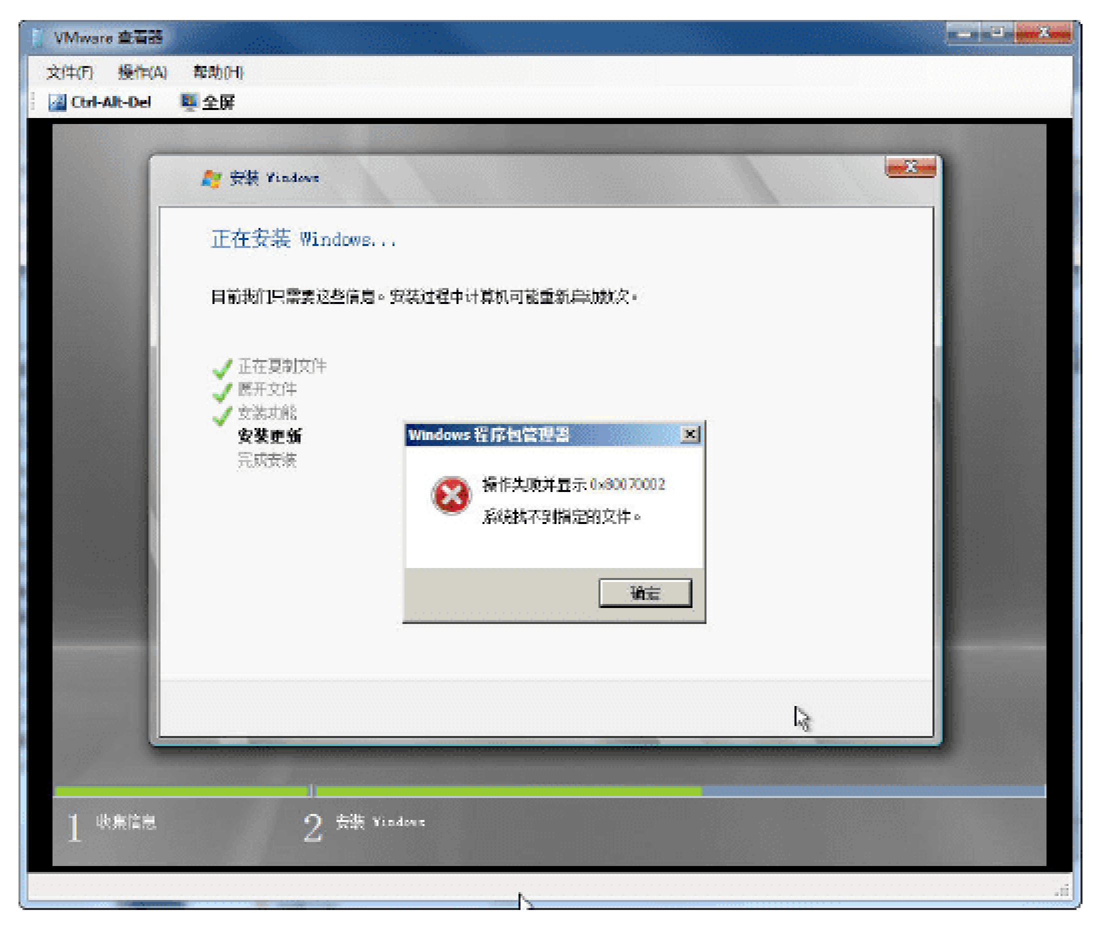


图 15-58　出现 0x80070002 错误

此时，部署 Windows 7、Hyper-V Server 2008 R2 的时候，也会出现该错误提示。

这个问题的原因是，在“Windows 部署服务”中，使用的是原来 Windows Server 2008 的“启动映像”，而不是使用 Windows Server 2008 R2 的新的启动映射。此时，只需要在“Windows 部署服务→启动映像”中，添加最新的 Windows Server 2008 R2 及 Windows 7 SP1 的 x86 的映像，就可

以解决问题，如图 15-59 所示。

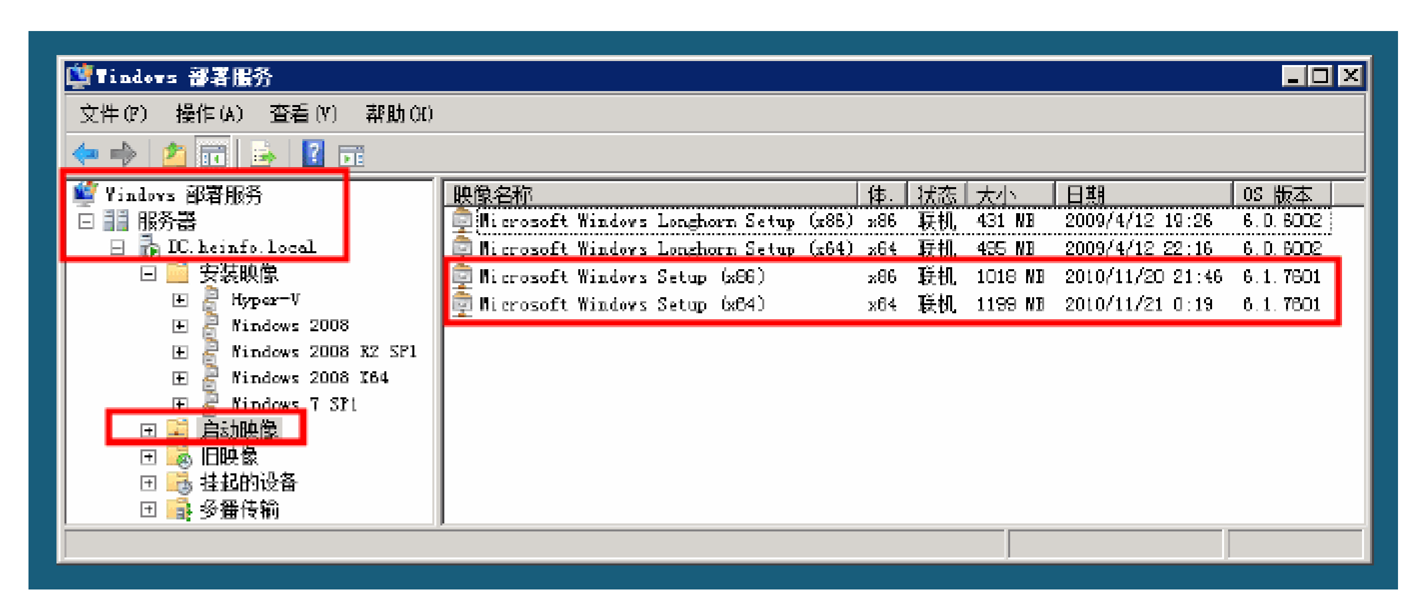


图 15-59　添加新版启动映像

说 明

Windows Vista 与 Windows Server 2008 使用同一内核，而 Windows Server 2008 R2 则与 Windows 7 使用同一内核。所以，只需要添加 Windows Server 2008（或 Windows Vista）、Windows Server 2008 R2（或 Windows 7）的启动映像即可。另外，Windows Server 2008 R2 只有 64 位产品，如果要部署 32 位的 Windows 7，则需要添加 32 位的 Windows 7 的启动映像。

添加启动映射之后，在使用“Windows 部署服务”远程安装操作系统，选择操作系统选单的时候，如果部署的是 Windows Vista 及 Windows Server 2008，可以选择“Microsoft Windows Longhorn Setup”，也可以选择“Microsoft Windows Setup”，如果要部署 Windows 7 及 Windows Server 2008 R2，则需要选择新添加的“Microsoft Windows Setup”，如图 15-60 所示。

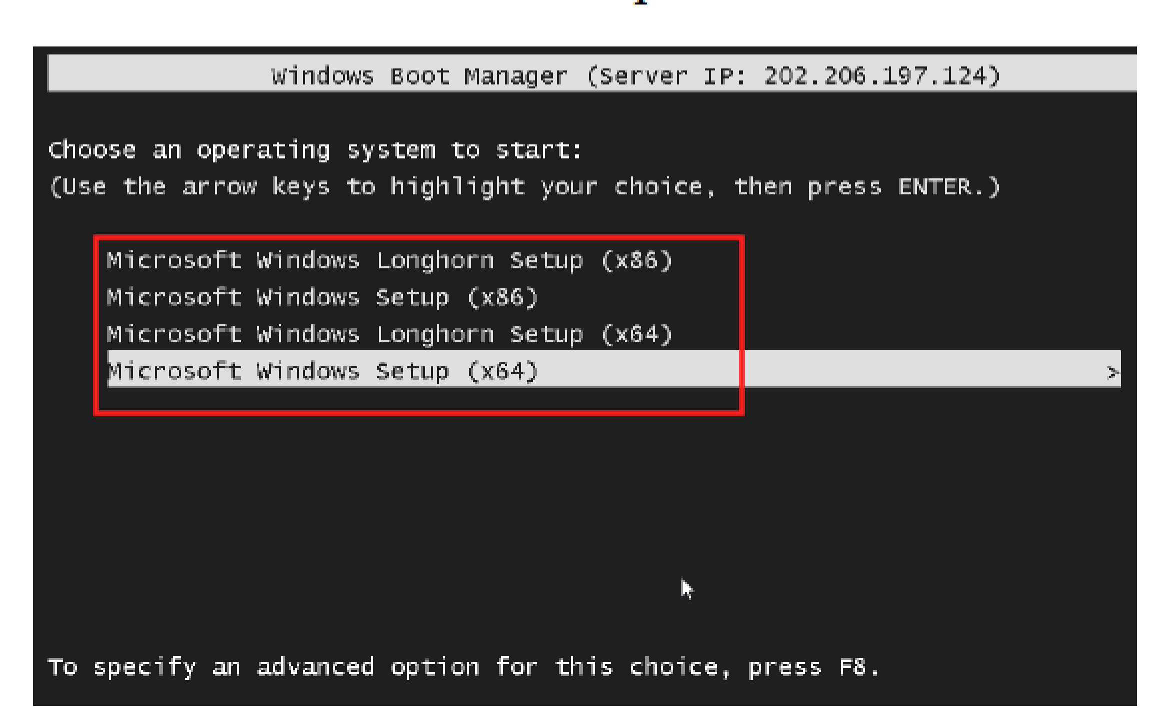


图 15-60　启动选单

第 16 章　Forefront TMG 2010 系统管理与应用

Forefront TMG 是 Microsoft 第 1 个 64 位的防火墙与代理服务器软件，它只支持 Windows Server 2008 操作系统。Forefront TMG 继承并发扬了 ISA Server 的功能与特点，并且增加了许多新的功能。本章主要介绍了使用 Forefront TMG 配置成使用 PPTP 与 L2TP 协议的“标准”VPN 服务器的组建，还介绍了适合 Windows Vista、Windows 7 等客户端使用的 SSTP 协议的 VPN 服务器的组建。

本章介绍使用 Microsoft Forefront TMG 2010 做防火墙、代理服务器、VPN 服务器的内容，其中 VPN 部分还包括组建基于传统 PPTP、L2TP 协议的 VPN 网络，以及包括 Microsoft 最新的基于 SSTP 协议的 VPN 网络的组建。同时，还介绍使用 Forefront TMG 为多个站点组建 VPN 路由的方式，让 Forefront TMG 轻松连接多个广域网。为了让大家快速入门，本章将以 4 个案例的方式进行介绍。

（1）案例 1：16.1～16.4 节。介绍 Forefront TMG 的基本使用，在这些内容中，介绍的是“案例 1”，即使用 Forefront TMG 做防火墙与代理服务器。

（2）案例 2：16.5 节。介绍基于 PPTP、L2TP 协议的 VPN 服务器的组建，是在“案例 1”的基础上，使用同一台服务器组建的 VPN 服务器。

（3）案例 3：16.6 节。介绍 VPN 路由器的配置，是在“案例 2”的基础上，通过连接另外一个远程网络来实现的。

（4）案例 4：16.7 节。介绍基于 SSTP 协议的 VPN 服务器的组建，是在“案例 1”的基础上，通过增加 Windows Server 2008 的“证书服务器”进行配置来实现的。

16.1　Forefront TMG 功能概述

Forefront TMG 是 Forefront Threat Management Gateway 的简称，它是 Microsoft 推出的最新一代的集防火墙、代理服务器、入侵检测、安全网关于一体的安全产品，相对于它的上一个版本 ISA（是 Internet Security and Acceleration 的简称）Server 2006，它属于全新的架构：只支持 64 位平台并且需要 Windows Server 2008（及其以上）的操作系统。它具有更好的性能、更高的安全性。

Forefront TMG 的构建基础是 Microsoft Internet Security and Acceleration（ISA）Server，旨在提供完善的集成网络安全网关。 在 Forefront TMG 方面进行的主要投资旨在提供其他保护功能，以确保公司网络能够抵御基于 Internet 的外部威胁。

16.1.1　Forefront TMG 的功能

它包括以下新功能：

（1）Web 反恶意软件，它是 Forefront TMG Web 保护订阅服务的一部分。 Web 反恶意软件可扫描网页以查找病毒、恶意软件和其他威胁。

（2）URL 筛选，根据 URL 类别（例如色情内容、毒品或购物）允许或拒绝访问网站。不仅可以阻止员工访问包含已知恶意软件的网站，还可通过限制或阻止访问干扰网站来确保业务效率。 URL 筛选也是 Web 保护订阅服务的一部分。

（3）电子邮件保护订阅服务，Forefront TMG 基于 Forefront Protection 2010 for Exchange Server 中的集成技术，来提供电子邮件保护订阅服务。Forefront TMG 可作为 SMTP 通信中继，并且可以扫描网络电子邮件以查找病毒、恶意软件、垃圾邮件和内容（例如可执行文件或加密的文件）。

（4）HTTPS 检查，可检查 HTTPS 加密会话，以确定是否存在恶意软件或漏洞利用情况。出于隐私考虑，可以不对特定网站组（如银行网站）进行检查。进行此项检查时会通知 Forefront TMG 客户端用户。

（5）网络检查系统（NIS），可检查通信，以确定是否存在利用 Microsoft 漏洞的情况。 NIS 可根据协议分析阻止各类攻击，并在最大程度上减少误报情况。 可以根据需要更新保护措施。

（6）增强的网络地址转换（NAT），能够指定可基于 1 对 1 NAT 发布的单个电子邮件服务器。

（7）增强的 Voice over IP 支持 SIP 遍历，允许在网络内简化 Voice over IP 的部署过程。

（8）支持 64 位的 Windows Server 2008，Forefront TMG 需要 64 位平台，并只能安装在 64 位的 Windows Server 2008 及 Windows Server 2008 R2 上。ISA Server 2006 不支持 Windows Server 2008，也不能安装在 64 位系统上。

16.1.2　Forefront TMG 版本

和 ISA Server 2006 相似，Forefront TMG 2010 也包括标准版与企业版。这两个版本包含相同的功能，并且具有相同的保护和访问控制功能，只是支持的网络规模不同，表 16-1 显示了 Forefront TMG 标准版与企业版的功能以及不同之处。

表 16-1　Forefront TMG 标准版与企业版的区别

	标准版	企业版
支持的部署方案	单台服务器	独立陈列中的服务器
CPU 数量支持	最多 4 个 CPU	无限制
存储	本地	支持对防火墙策略和配置进行远程管理
陈列/NLB/CARP 支持	不支持，一个陈列中只能具有一台服务器	支持
企业管理	不支持	支持，增加了管理标准版的功能
是否支持发布“服务器”	支持	支持
是否支持 VPN	支持	支持
转发代理/缓存压缩	支持	支持
网络 IPS（NIS）	支持	支持
电子邮件保护	支持，需要 Exchange 许可	支持，需要 Exchange 许可
Web 保护	需要订阅	需要订阅
ISP 冗余功能	支持	支持

16.1.3 Forefront TMG 系统需求

Forefront TMG 需要最低 1.86GHz、双核、64 位 CPU（不需要硬件辅助虚拟化）、最低 4GB 内存（2GB 内存也可以运行，但较慢）、至少 2.5GB 的可用空间（必须是 NTFS 文件系统）用于安装（但 Forefront TMG 在运行过程中产生的日志比较大）、至少 1 个网卡（但一般至少 2 个网卡，带外围网络则需要 3 块甚至更多网卡）。

Forefront TMG 需要 64 位的 Windows Server 2008，也支持 Windows Server 2008 R2（只有 64 位版本），Forefront TMG 还需要 Windows Server 2008 中的“网络策略服务器”、“路由和远程访问服务”、Microsoft .Net Framework 3.5 SP1 等产品，这些软件可以由 Forefront TMG 准备工具进行安装。

16.2 Forefront TMG 部署与基本配置

本节将讲述 Forefront TMG 的安装与基本配置。在本节的内容中，将 Forefront TMG 安装在一台具有 2GB 内存、安装了 Windows Server 2008 R2 中文版操作系统、具有两个网卡的计算机上。

16.2.1 多 VLAN 网络中三层交换机的配置

一些人对软件防火墙有个错误的概念，认为软件防火墙不能支持多网段，实际上是没有了解网络、路由、网关的概念及意义导致的误解。如果让软件防火墙支持多网段，除了需要在网络中的三层交换机上设置静态路由外，还要在安装软件防火墙的计算机上使用 route 命令，添加到其他网段的静态路由。为了让大家明了，本节通过具体的实例，介绍这个问题。

某单位网络，有大约 400 台计算机，10 几台服务器，一条 20M 的光纤连接到 Internet。在该单位中，通过一台高端的华为交换机作核心交换机，其他若干台交换机做接入层交换机。如图 16-1 所示。

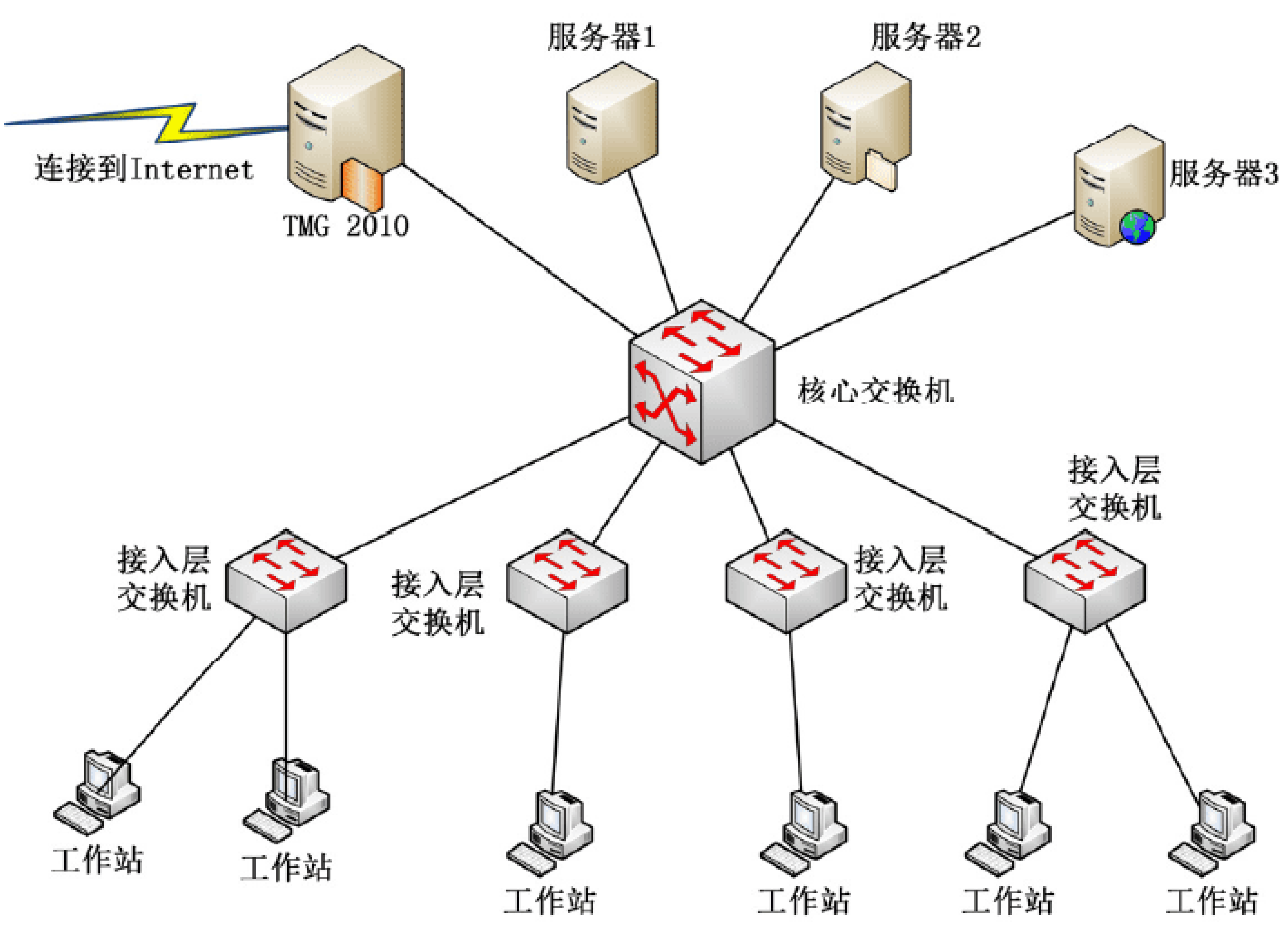


图 16-1 Forefront TMG 网络案例

整个网络，划分了 12 个网段，其中：

将 400 台计算机，根据楼层、部门的不同，划分为 10 个 VLAN，VLAN 的标记从 VLAN11、VLAN12～VLAN20，这些网段采用 192.168.1.0/24、192.168.2.0/24、192.168.3.0/24～192.168.10.0/24 的地址，网关地址是每个网段的最后一个地址，例如，对于 VLAN11，其网关地址是 192.168.1.254。

所有的服务器（Forefront TMG 除外）使用一个网段，划分为 VLAN100，该网段采用 192.168.100.0/24 的地址，网关地址为 192.168.100.254。

对于 Forefront TMG，专门使用一个网段，划分为 VLAN200，该网段采用 192.168.254.0/24 的地址，网关地址是 192.168.254.254。设置 Forefront TMG 的内网地址为 192.168.254.252/24，则需要在“核心交换机”上，添加指向 192.168.254.252 的静态路由，内容如下：

```
vlan 200
desc "moren wangguan"
port e0/24
inte vlan 200
ip   addr   192.168.254.254    255.255.255.0
ip   route-static   0.0.0.0   0.0.0.0    192.168.254.252
```

在上面的设置中，设置端口 24 为 192.168.254.0 网段，设置默认路由到 192.168.254.252。

16.2.2　在计算机上添加到其他网段的静态路由

在计算机上添加到其他网段的静态路由，主要步骤如下。

01 在将要安装 Forefront TMG 的计算机上安装两块网卡：一块网卡连接 Internet，设置网卡名称为 wan；另一块网卡连接内网，设置网卡名称为 lan，如图 16-2 所示。

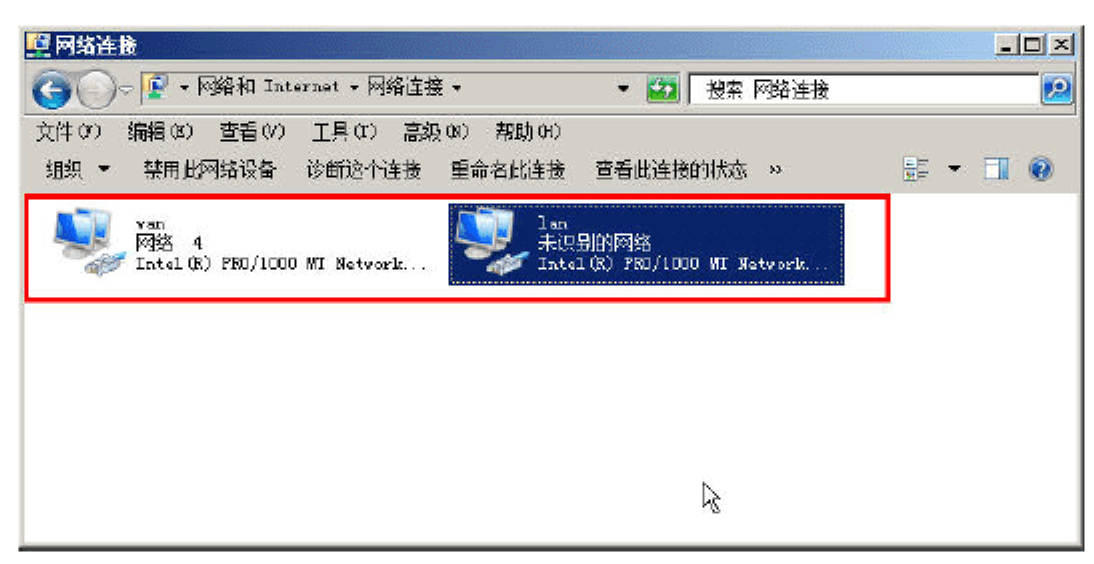


图 16-2　重命名网卡



说 明

可以在“控制面板→网络和共享中心”中，通过单击“更改适配器设置”，打开“网络连接”页。

02 将连接 Internet 的网卡，设置公网地址、子网掩码并设置其网关地址（在本示例中，这个公网地址为 202.206.197.125，子网掩码为 255.255.255.224，网关地址为 202.206.197.97），如图 16-3 所示。

03 设置完公网地址以后，进入“命令提示符”，执行 ping 命令，测试到网关的连通性，如图 16-4 所示。

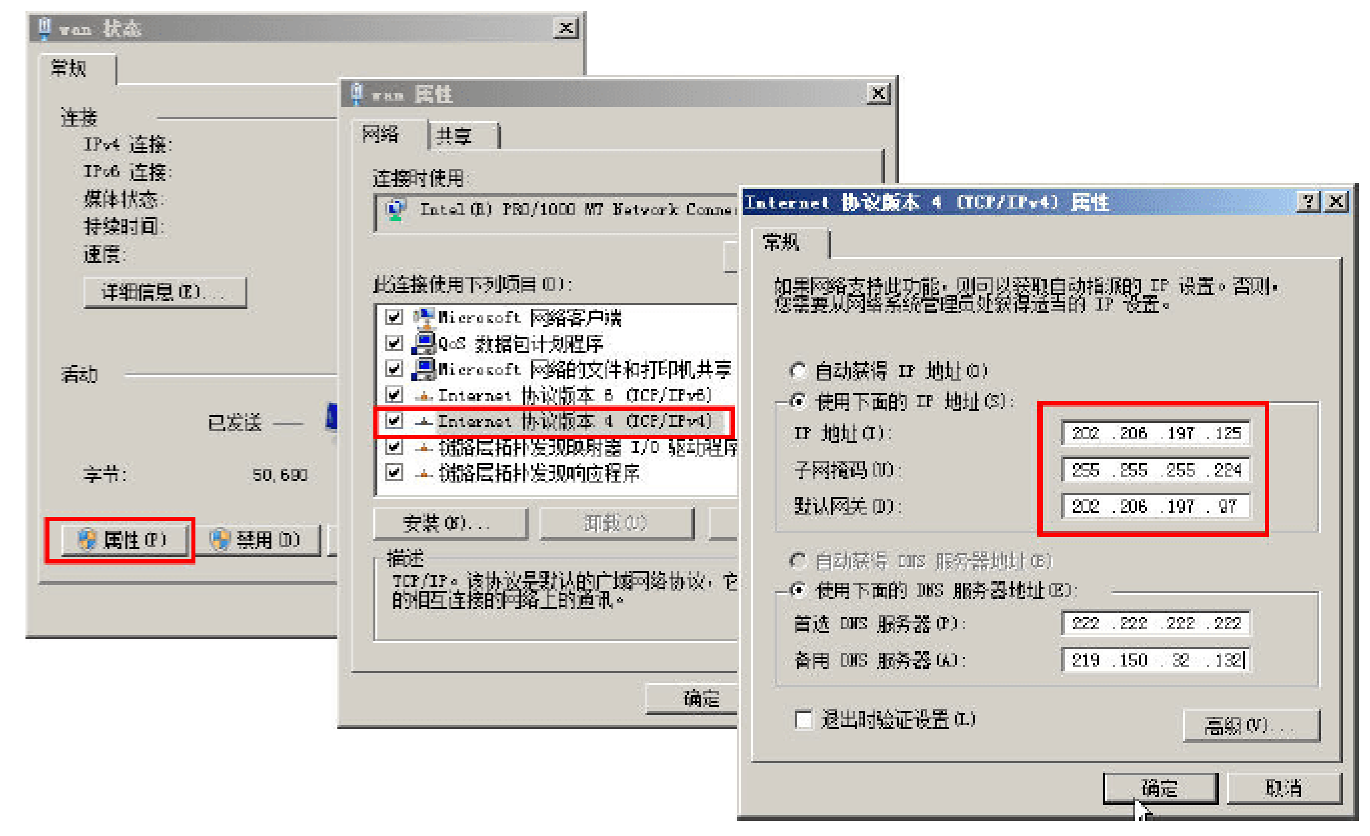




图 16-3　设置公网地址



图 16-4　测试网络连通性

当网络连通之后，继续后面的操作。

04 将连接局域网的网卡，设置内网地址、子网掩码。在本例中，IP 地址为 192.168.254.252、子网掩码为 255.255.255.0，不需要设置网卡地址，如图 16-5 所示。

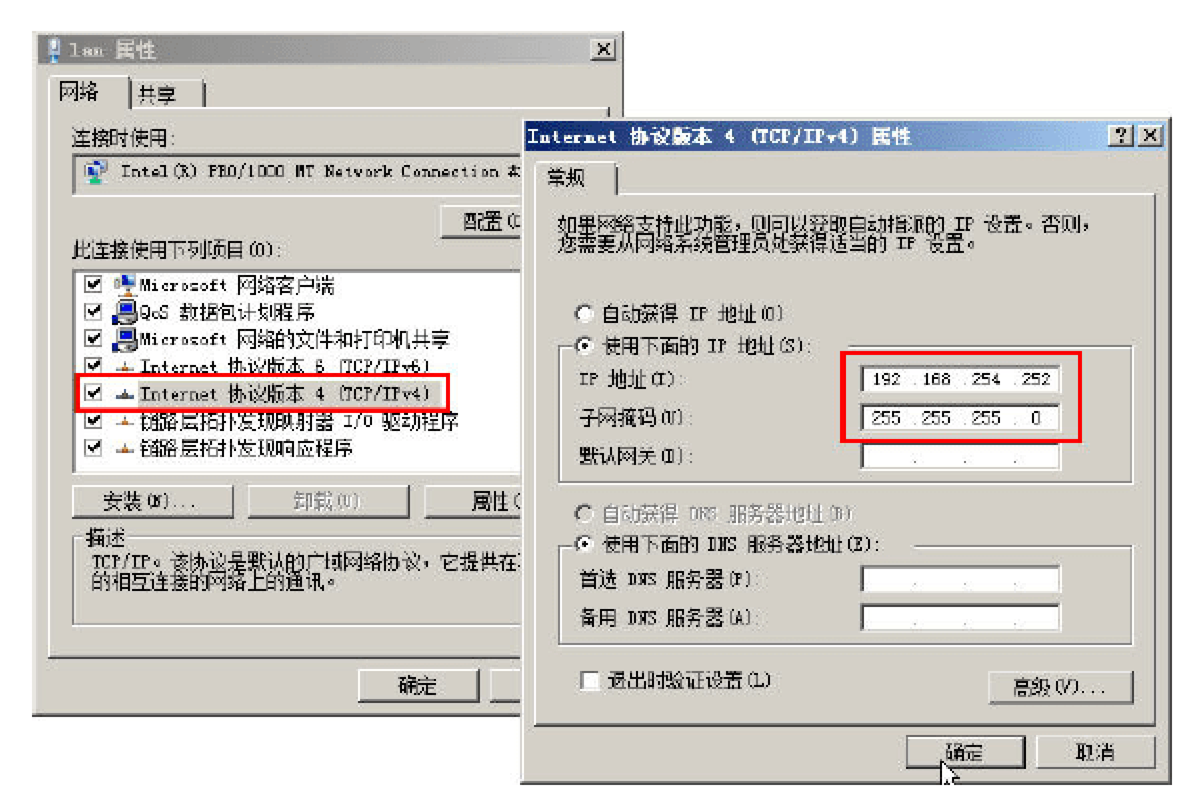


图 16-5　设置内网地址

05 为了让 192.168.254.252 可以访问其他子网，需要在命令提示符中添加到其他 VLAN 的静态路由，其命令格式如下：

```
route   -p   add   192.168.1.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.2.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.3.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.4.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.5.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.6.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.7.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.8.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.9.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.10.0     mask   255.255.255.0     192.168.254.254
route   -p   add   192.168.100.0     mask   255.255.255.0     192.168.254.254
```

06 在计算机上运行一次这些命令即可，在运行之后，可以使用 route print 命令查看添加的

静态路由，如图 16-6 所示。

永久路由:

网络地址	网络掩码	网关地址	跃点数
0.0.0.0	0.0.0.0	202.206.197.97	默认
192.168.1.0	255.255.255.0	192.168.254.254	1
192.168.2.0	255.255.255.0	192.168.254.254	1
192.168.3.0	255.255.255.0	192.168.254.254	1
192.168.4.0	255.255.255.0	192.168.254.254	1
192.168.5.0	255.255.255.0	192.168.254.254	1
192.168.6.0	255.255.255.0	192.168.254.254	1
192.168.7.0	255.255.255.0	192.168.254.254	1
192.168.8.0	255.255.255.0	192.168.254.254	1
192.168.9.0	255.255.255.0	192.168.254.254	1
192.168.10.0	255.255.255.0	192.168.254.254	1
192.168.100.0	255.255.255.0	192.168.254.254	1

图 16-6　添加的静态路由

16.2.3　Forefront TMG 的安装

完成上面的配置后，接下来开始安装 Forefront TMG，主要步骤如下。

01 检查无误后，将 Forefront TMG 标准版安装光盘放入光驱中，开始 Forefront TMG 标准版的安装。在安装程序界面中，单击“运行准备工具”链接 ，如图 16-7 所示。



图 16-7　安装 Forefront TMG

02 在“欢迎使用 Microsoft Forefront Threat Management Gateway（TMG）准备工具”对话框中，单击“下一步”按钮，如图 16-8 所示。

03 在“许可协议”对话框中，选中“我接受许可协议中的条款”复选框，然后单击“下一步”按钮，如图 16-9 所示。

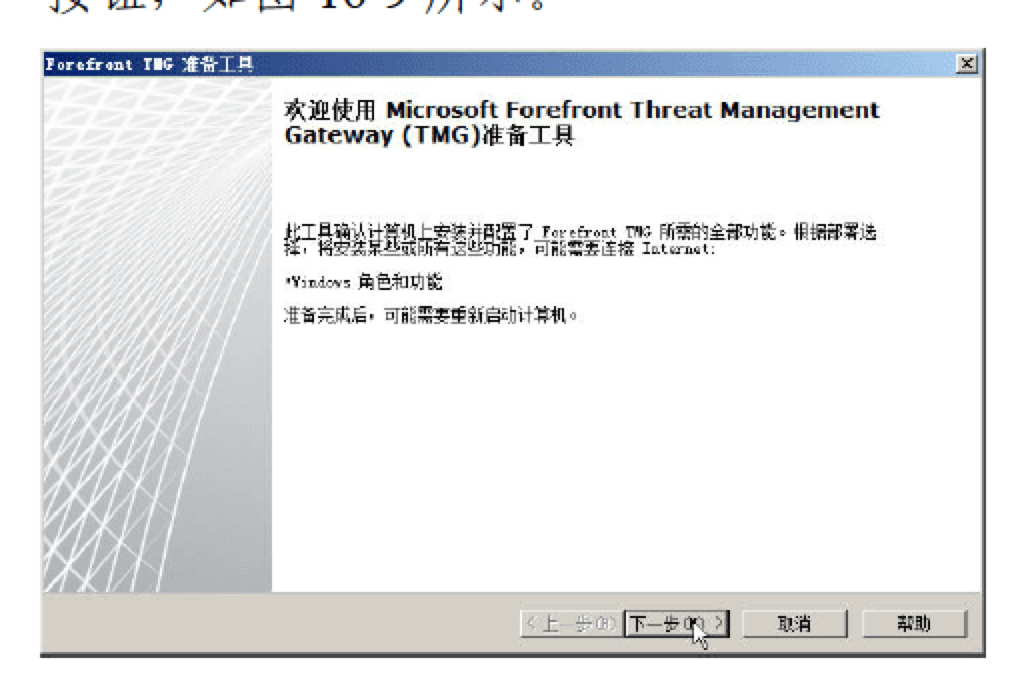


图 16-8　准备工具

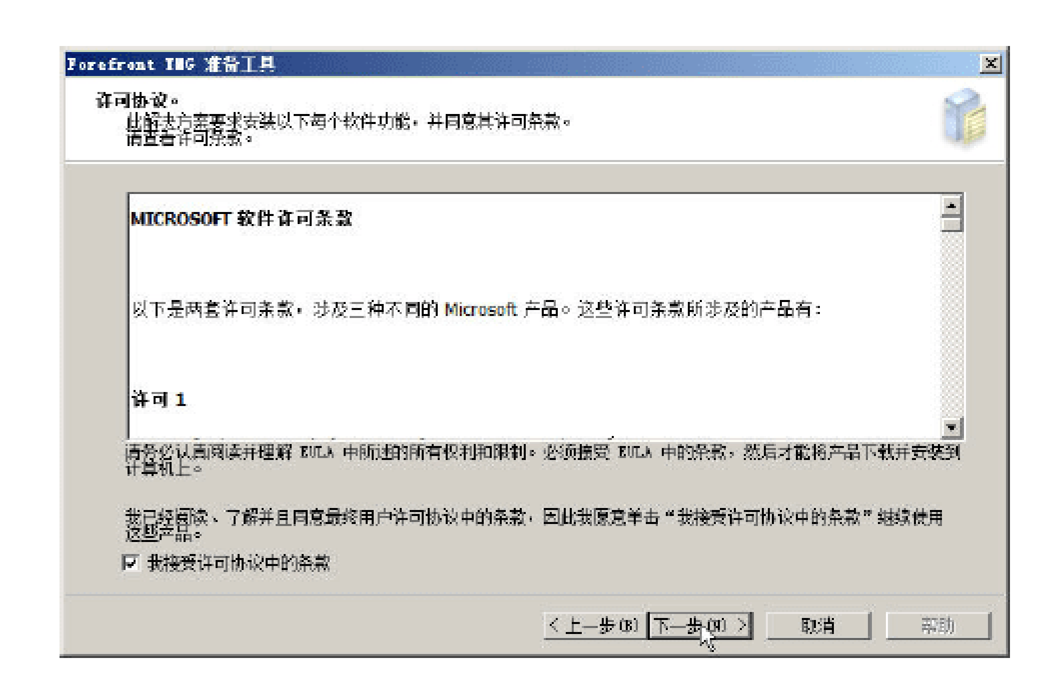


图 16-9　接受许可协议

04 在“安装类型”对话框中，选中“Forefront TMG 服务和管理”单选按钮，如图 16-10 所示。

05 随后，准备工具将在计算机上安装必备的组件，这需要从 Microsoft 网站下载相关的软件。所以这时候，要求当前计算机能访问 Internet。如果不能访问 Internet，准备工具会失败退出。

06 如果一切正常，大约几分钟内，准备工具会完成，如图 16-11 所示。

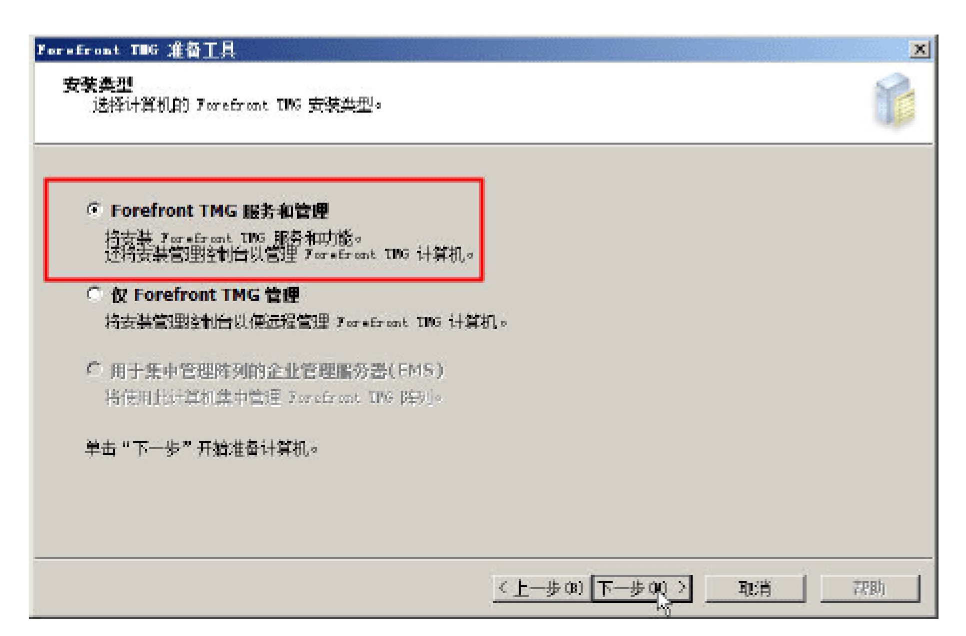


图 16-10　安装 TMG 服务和管理工具

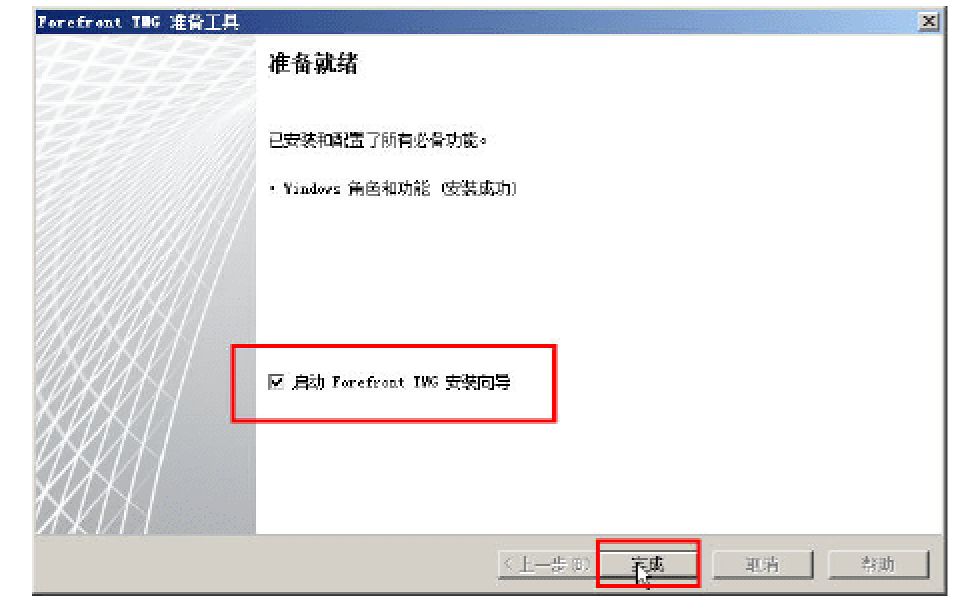


图 16-11　准备工具完成

07 在运行完准备工具之后，会进入 Forefront TMG 的安装向导，如图 16-12 所示。

08 在“许可协议”对话框中，选中“我接受许可协议中的条款”单选按钮，如图 16-13 所示。

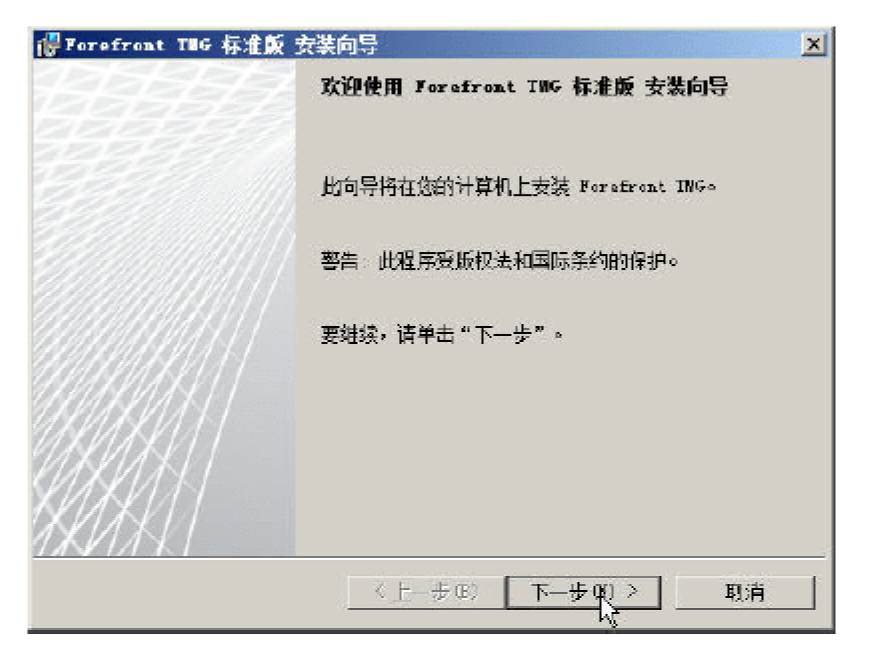


图 16-12　Forefront TMG 安装向导



图 16-13　接受许可协议

09 在“客户信息”对话框中，输入用户名、单位名称和 Forefront TMG 产品序列号，如图 16-14 所示。

10 在“安装路径”对话框中，显示了 Forefront TMG 的安装路径，一般选择默认值即可，如图 16-15 所示。

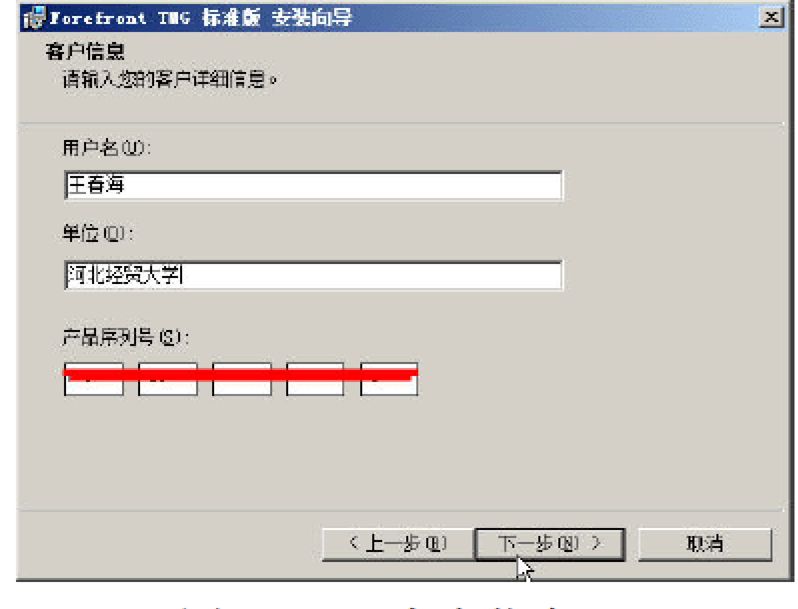


图 16-14　客户信息

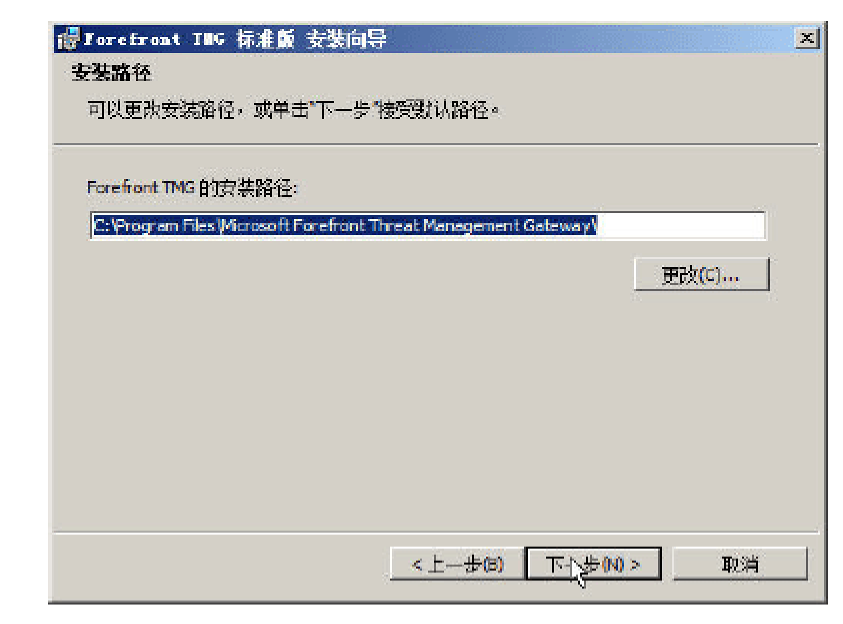


图 16-15　安装路径

11 在“定义内部网络”对话框中，单击“添加”按钮，在打开的“地址”对话框中单击“添加适配器”按钮，在打开的“选择网络适配器”对话框中，选择连接内部局域网的网卡，在之前已

经将这个网卡重命名为“lan”，选中这个网卡并添加，如图 16-16 所示。

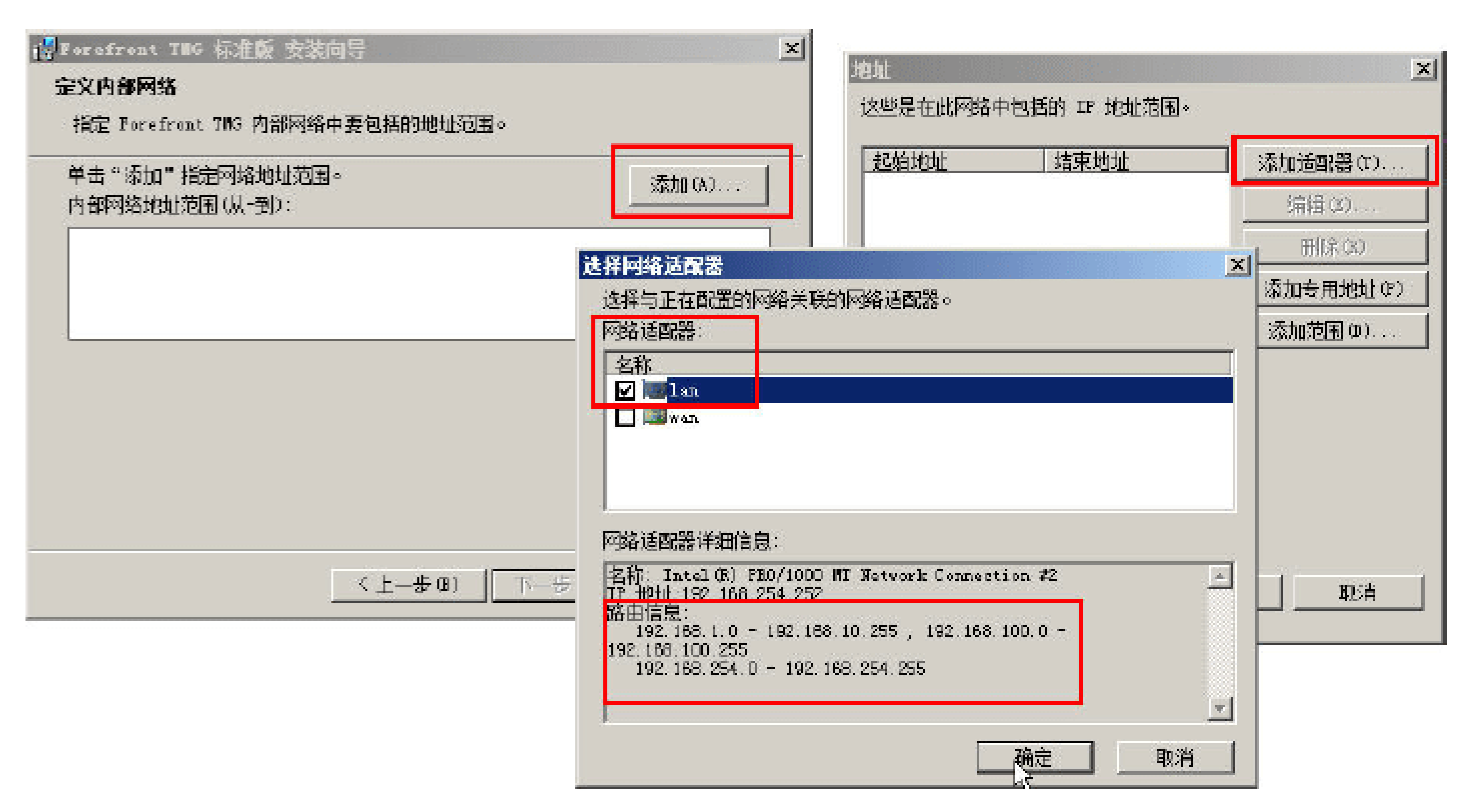
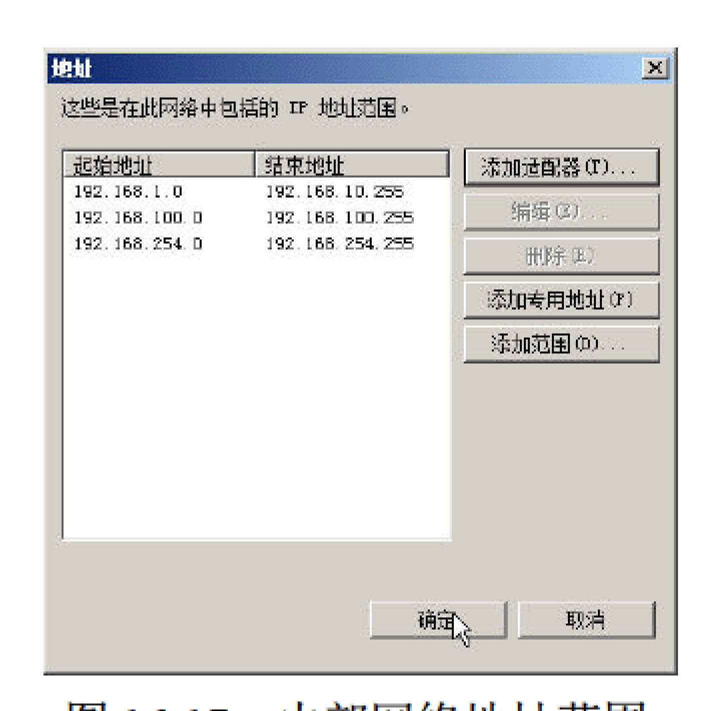


图 16-16　选择内部网卡

12 在“地址”对话框中，检查当前局域网内所有的子网地址是否已经添加。如果没有，单击“添加范围”按钮，在弹出的“IP 地址范围属性”对话框中，输入未添加的地址，然后单击“确定”按钮返回到“地址”对话框，如图 16-17 所示，单击“确定”按钮。

13 在“服务警告”对话框中单击“下一步”按钮。

14 在“为安装程序做好准备”对话框中，单击“安装”按钮，如图 16-18 所示。



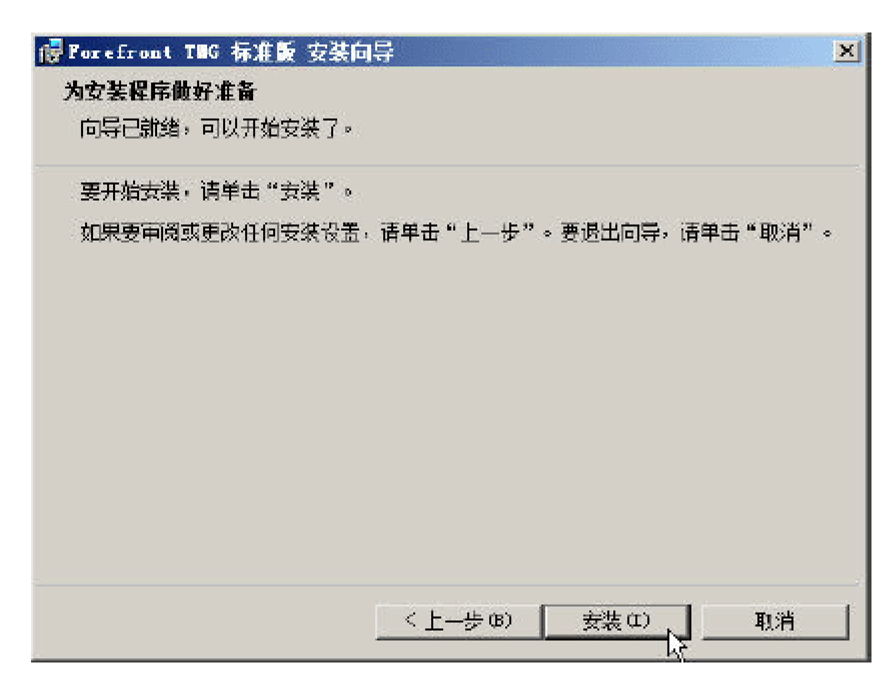


图 16-17　内部网络地址范围　　　　图 16-18　安装

15 在随后的过程中，Forefront TMG 将会安装，这大约会持续 30min 左右的时间，请耐心等待，如图 16-19 所示。

16 安装完成后，单击“完成”按钮，如图 16-20 所示。

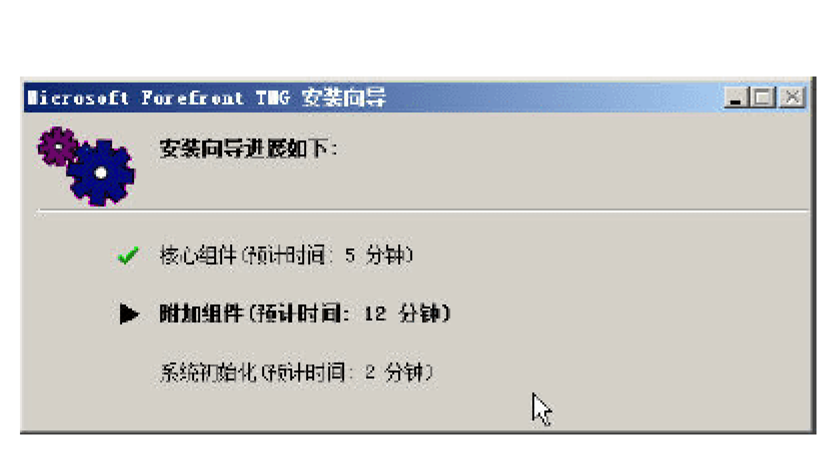




图 16-19　正在安装　　　　图 16-20　安装完成

16.3 Forefront TMG 入门向导

在 Forefront TMG 中，新增加了“入门向导”功能，可以让用户进行“网络设置”、“系统设置”，定义常用的部署选项。接下来将介绍这些功能。

16.3.1 网络设置向导

在第一次进入 Forefront TMG 管理工具时，Forefront TMG 入门向导会自动运行，如图 16-21 所示。

01 在“入门向导”对话框中，单击“配置网络设置”链接，进入网络设置对话框。

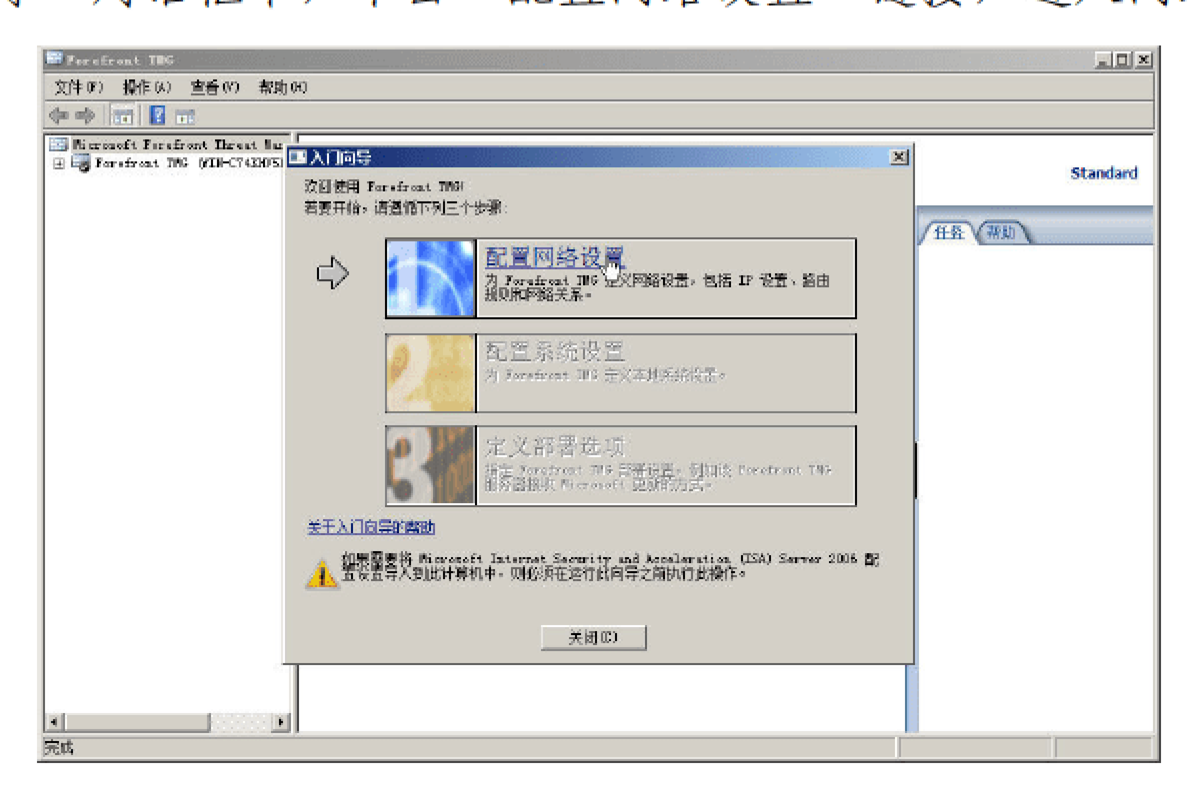


图 16-21 入门向导

02 在“网络模板选择”对话框中，选择适合的网络拓扑模板，如图 16-22 所示。在此，选中“边缘防火墙”单选按钮，这是最常用的一种网络拓扑。

03 在“局域网（LAN）设置”对话框中，选择连接到 LAN 的网络适配器，如图 16-23 所示。

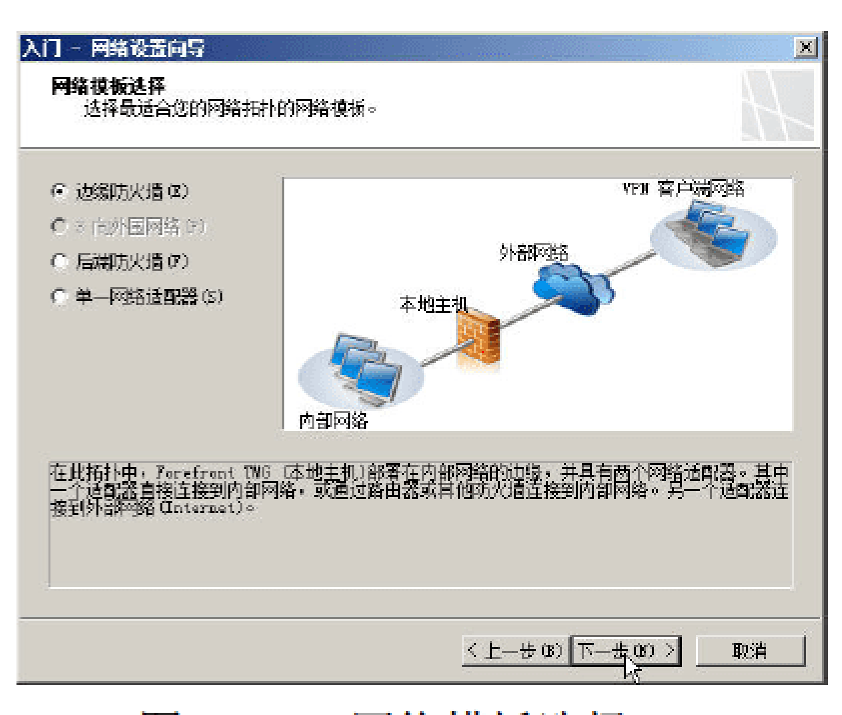


图 16-22 网络模板选择

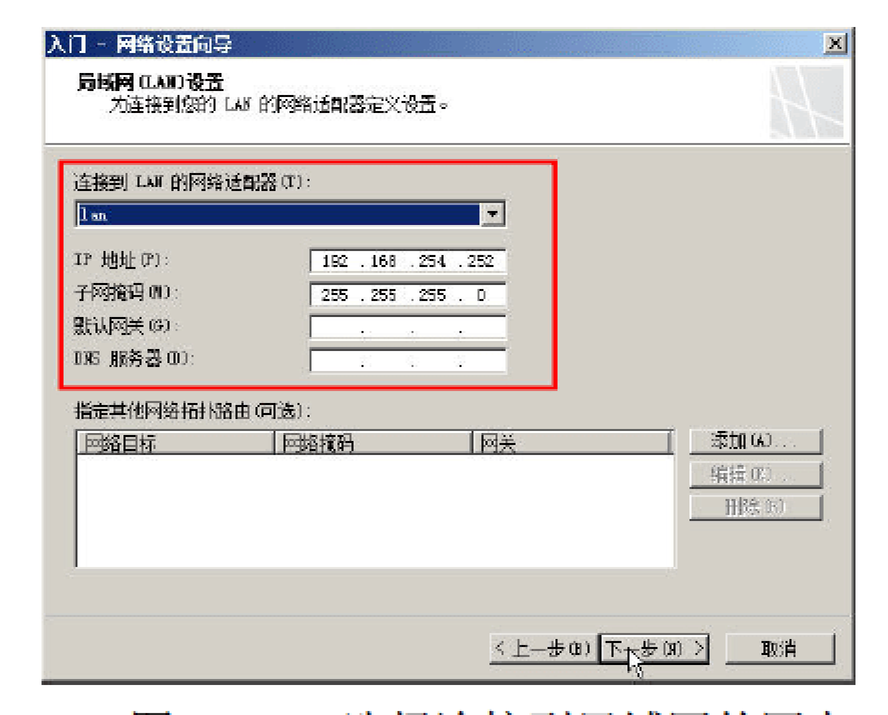


图 16-23 选择连接到局域网的网卡

说 明

在此设置中，可以单击“添加”按钮，添加到其他 VLAN 的静态路由。但是，这个功能有点小问题：如果已经在“命令提示符”中使用 route 命令添加了静态路由，就不需要在该界面中添加，否则会在“路由表”中生成重复的路由项；当然，如果没有使用 route 命令添加，则可以在该界面中添加到其他 VLAN 的静态路由。

04 在“Internet 设置”对话框中，选择连接到 Internet 的网络适配器，在此选择名为“wan”的网卡，如图 16-24 所示。

05 在“正在完成网络安装向导”对话框中，单击“完成”按钮，如图 16-25 所示。

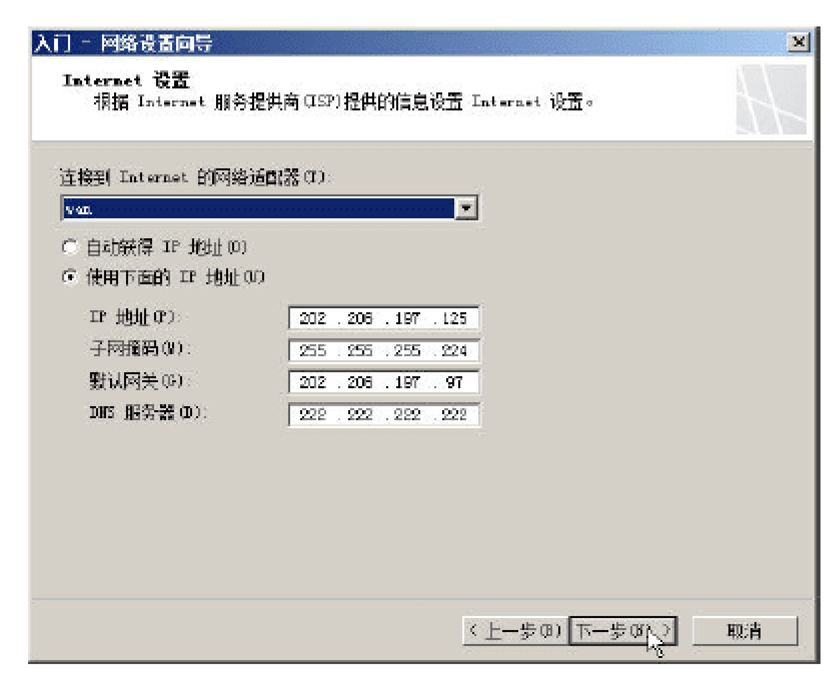


图 16-24　选择连接到 Internet 的网卡

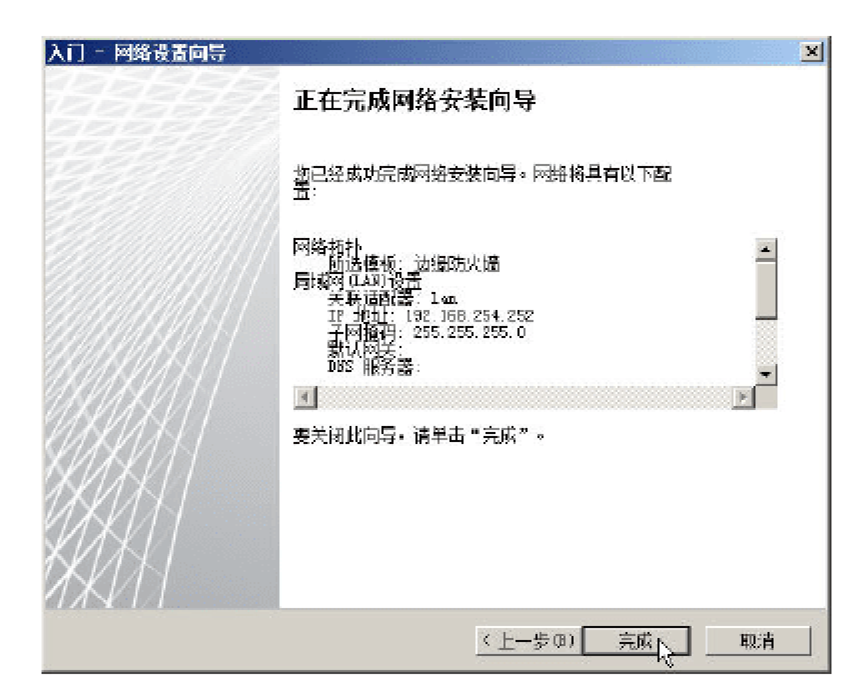


图 16-25　完成网络安装向导

16.3.2　系统设置向导

返回到“入门向导”对话框，单击“配置系统设置”链接，如图 16-26 所示。

01 在“主机标识”对话框中，可以更改计算机名称或者将计算机加入到域。在此修改计算机的名称为 TMG2010，其他保持不变，如图 16-27 所示。



图 16-26　配置系统设置

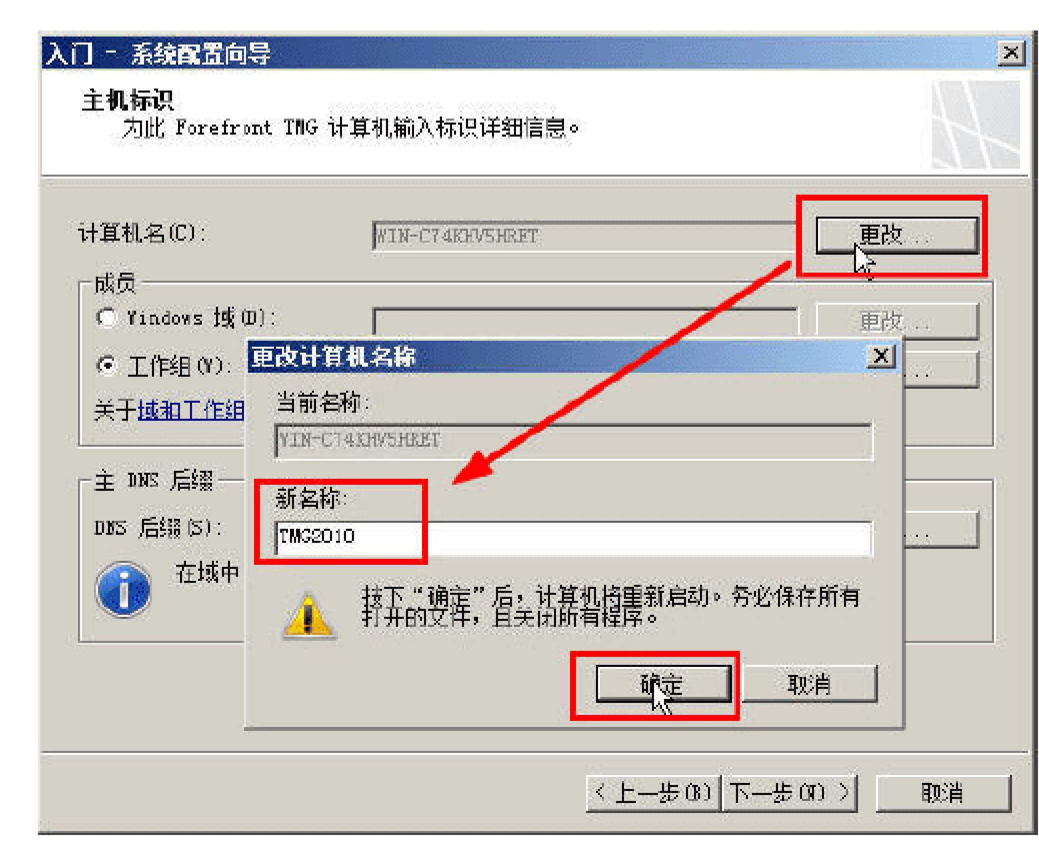


图 16-27　更改计算机名称

更改完计算机名称后，Forefront TMG 将会重新启动计算机。

02 再次进入系统后，定位到“开始→程序→所有程序”，进入“Microsoft Forefront TMG”程序组，运行“Forefront TMG 管理”程序。再次进入 Forefront TMG 后，在“入门向导”中单击“配置系统设置”链接，继续后面的步骤，如图 16-28 所示。

03 在“正在完成系统配置向导”对话框中，单击“完成”按钮，如图 16-29 所示。

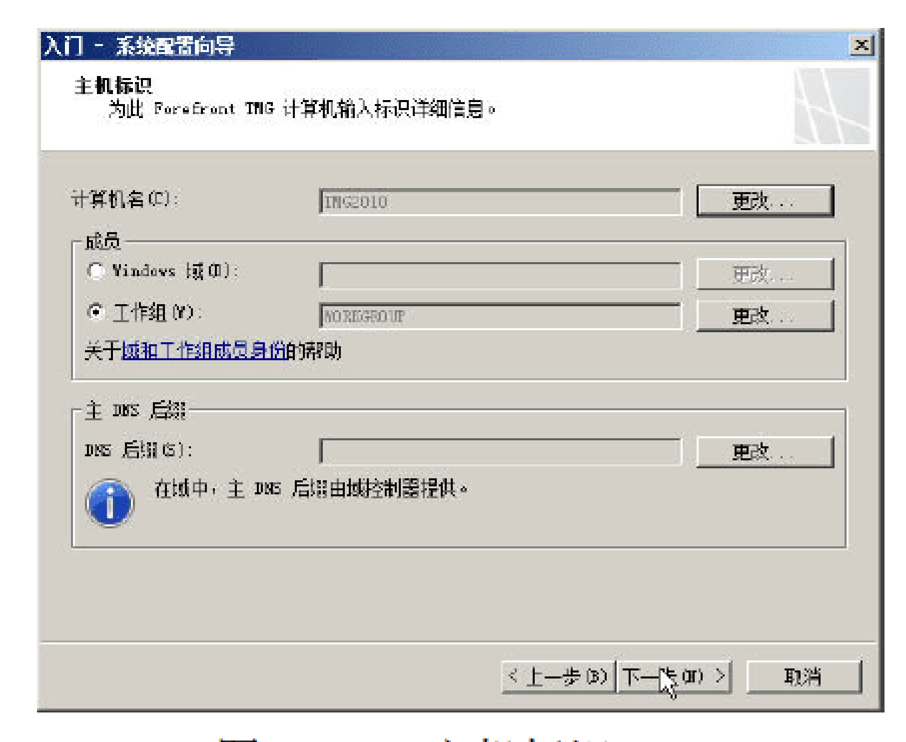




图 16-28　主机标识

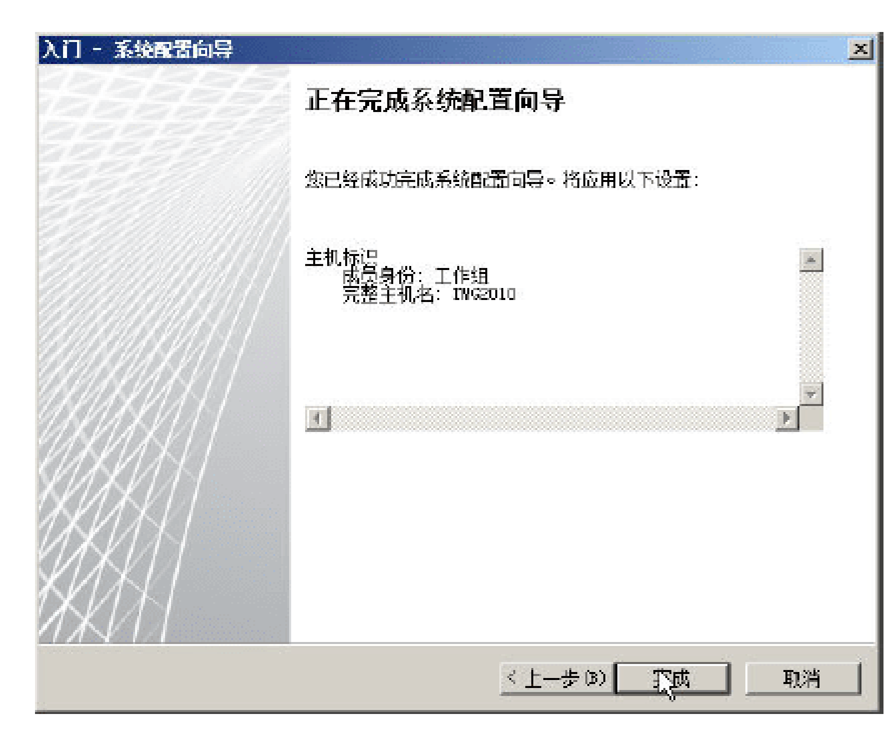


图 16-29　完成系统配置

16.3.3　部署选项

返回到“入门向导”对话框后，单击“定义部署选项”链接，如图 16-30 所示。

01 在“Microsoft Update 设置”对话框中，选中“使用 Microsoft Update 服务检查更新”单选按钮，如图 16-31 所示。



图 16-30　部署选项

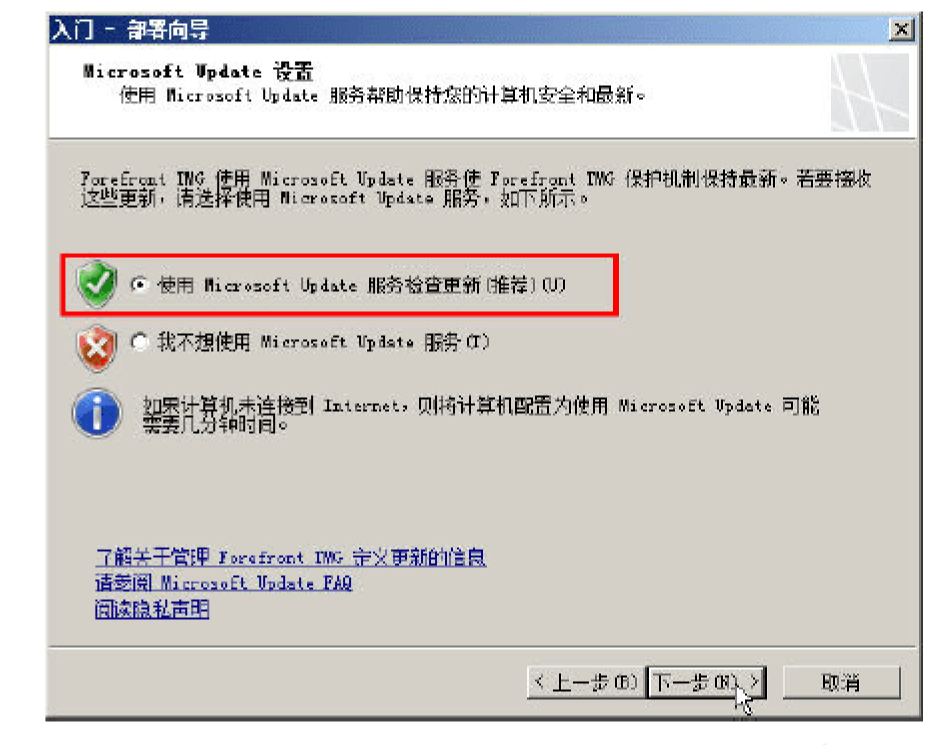


图 16-31　使用 Microsoft 更新服务

02 在“Forefront TMG 保护功能设置”对话框中，在“网络检查系统”选项组中，在“许可证”下拉列表中选择“激活补丁许可证并启用 NIS”选项；在“Web 保护”选项组中，在“许可证”下拉列表中选择“激活评估许可证并启用 Web 保护”选项，并选中“启用恶意软件检查”复选框，如图 16-32 所示。如果你有正式的许可证，也可以在此输入许可证编号；也可以在 Forefront TMG 管理控制台中，更新许可证编号。

03 在“NIS 签名更新设置”对话框中，选择默认值，如图 16-33 所示。

04 在“客户反馈”对话框中，根据实际情况，选择是否向 Microsoft 发送改善计划，如图 16-34 所示。

05 在“Microsoft 遥测报告服务”对话框中，选择参与级别，如图 16-35 所示。

06 在“正在完成部署向导”对话框中，单击“完成”按钮，如图 16-36 所示。

07 返回到“入门向导”对话框后，选中“运行 Web 访问向导”复选框，单击“关闭”按钮，如图 16-37 所示。



图 16-32　启用 NIS

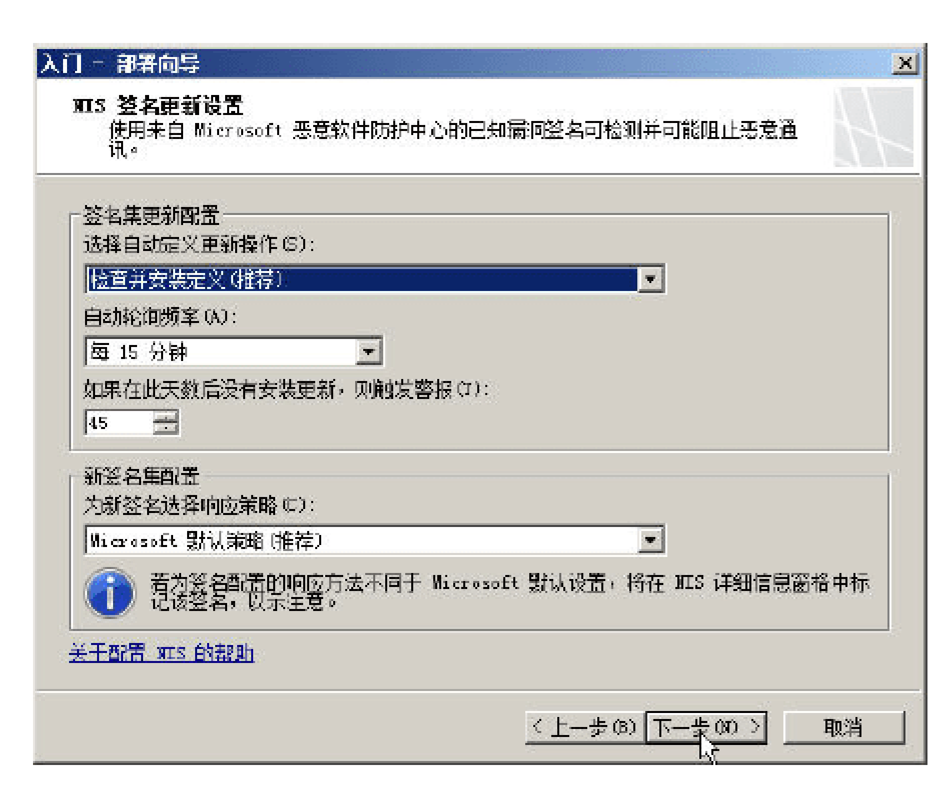


图 16-33　NIS 签名更新设置

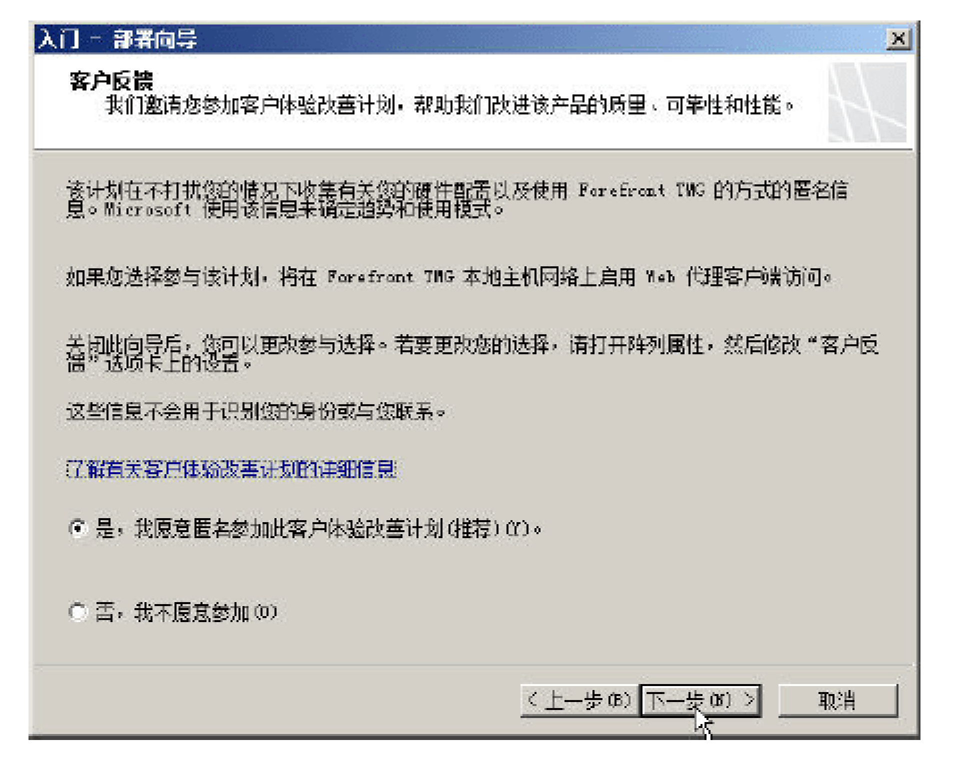


图 16-34　客户反馈

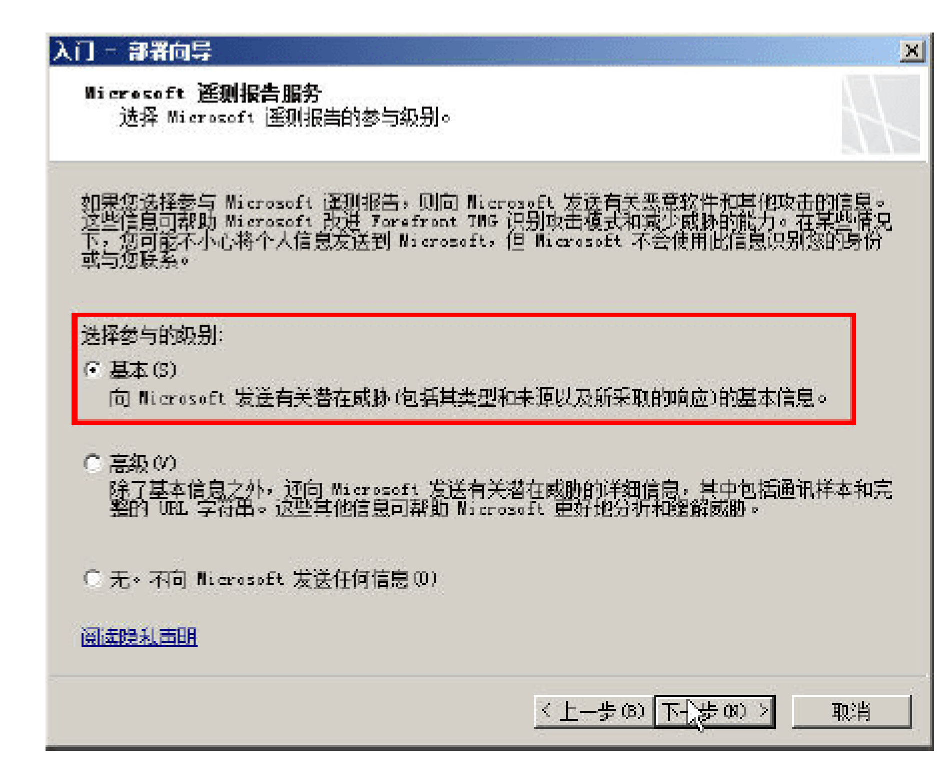


图 16-35　遥测参与级别

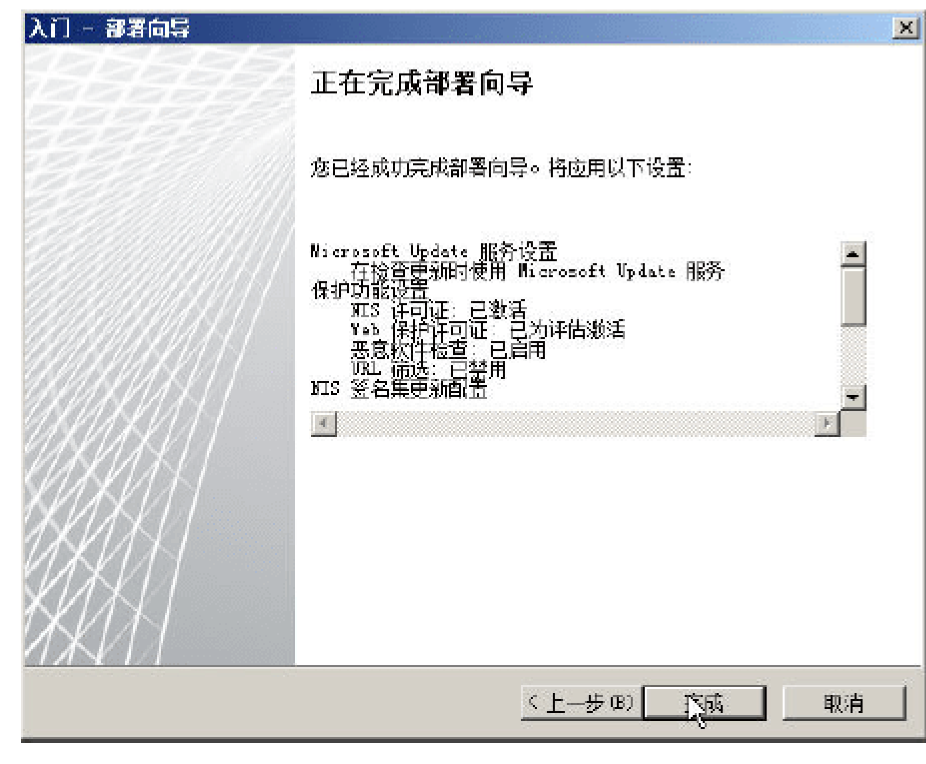


图 16-36　部署向导



图 16-37　完成入门向导

16.3.4　Web 访问向导

在关闭“入门向导”对话框的时候，如果选中“运行 Web 访问向导”复选框，则进入创建 Web 访问策略向导页，在该向导中可以定义“阻止的 Web 访问”、“阻止的 URL 类别和 Web 目标”、“恶意软件检查设置”、“HTTPS 检查设置”、“Web 缓存设置”等项。本节将介绍这些内容，其主要步骤如下。

01 在“欢迎使用 Web 访问策略向导”对话框中，单击“下一步”按钮，如图 16-38 所示。

02 在“Web 访问策略规则”对话框中，选中“是，创建规则来阻止推荐的最少 URL 类别”单选按钮，如图 16-39 所示。




图 16-38　Web 访问策略向导

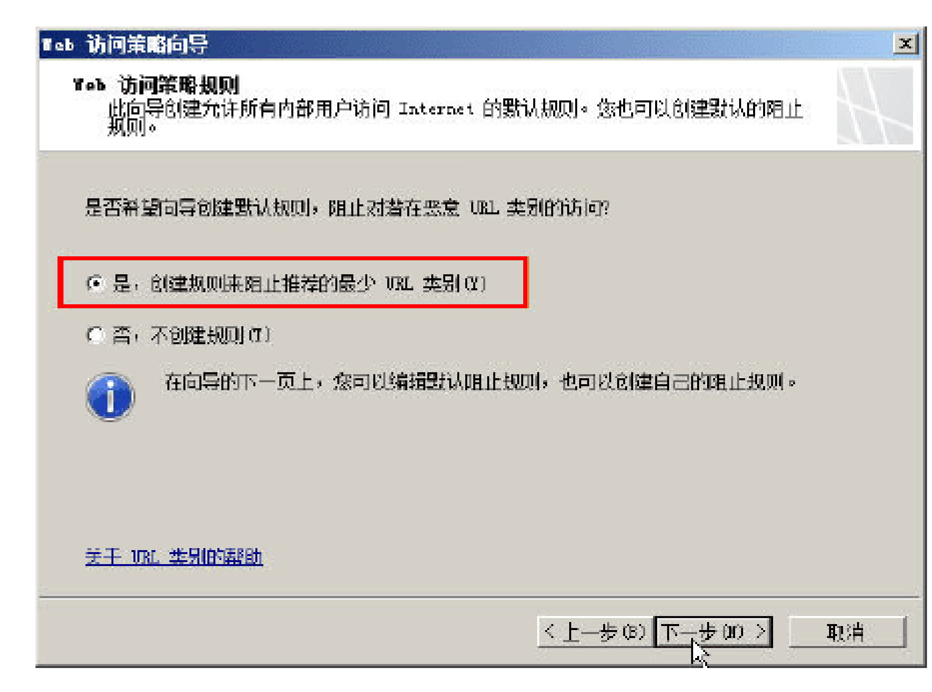


图 16-39　创建规则

03 在“阻止的 Web 目标”对话框中，选择要阻止的目标，一般情况下，选择默认值即可。如果要排除某些目标，则在“阻止对下列 Web 目标的访问”列表框中，选中并单击“删除”按钮。如图 16-40 所示。

04 在“恶意软件检查设置”对话框中，选择是否启用恶意软件检查。在此选中“是，检查从 Internet 请求的 Web 内容”单选按钮，如图 16-41 所示。

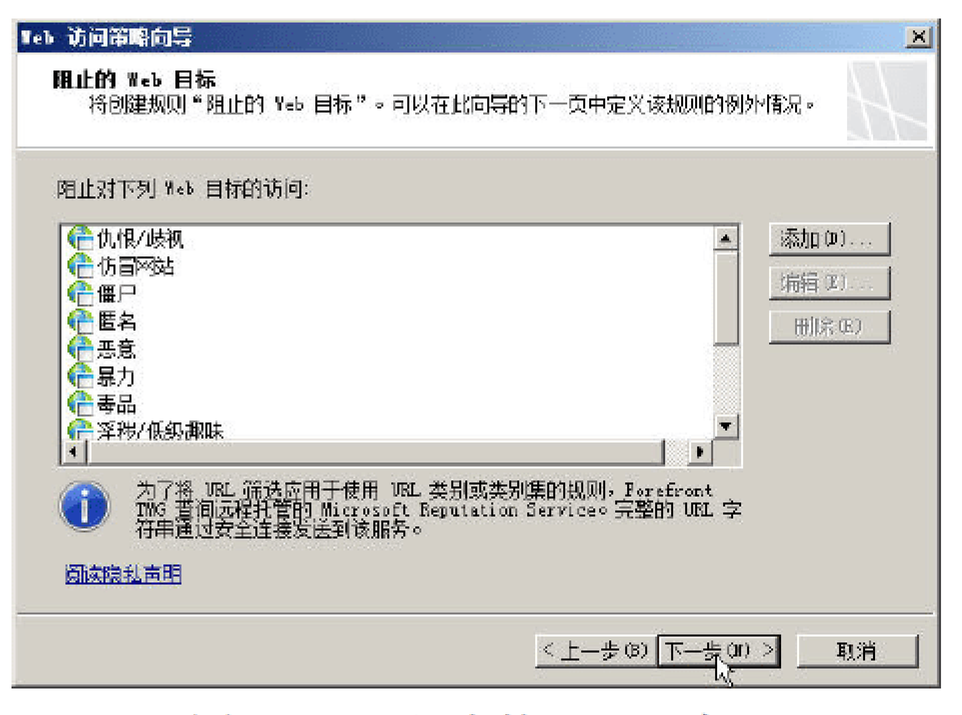


图 16-40　阻止的 Web 目标

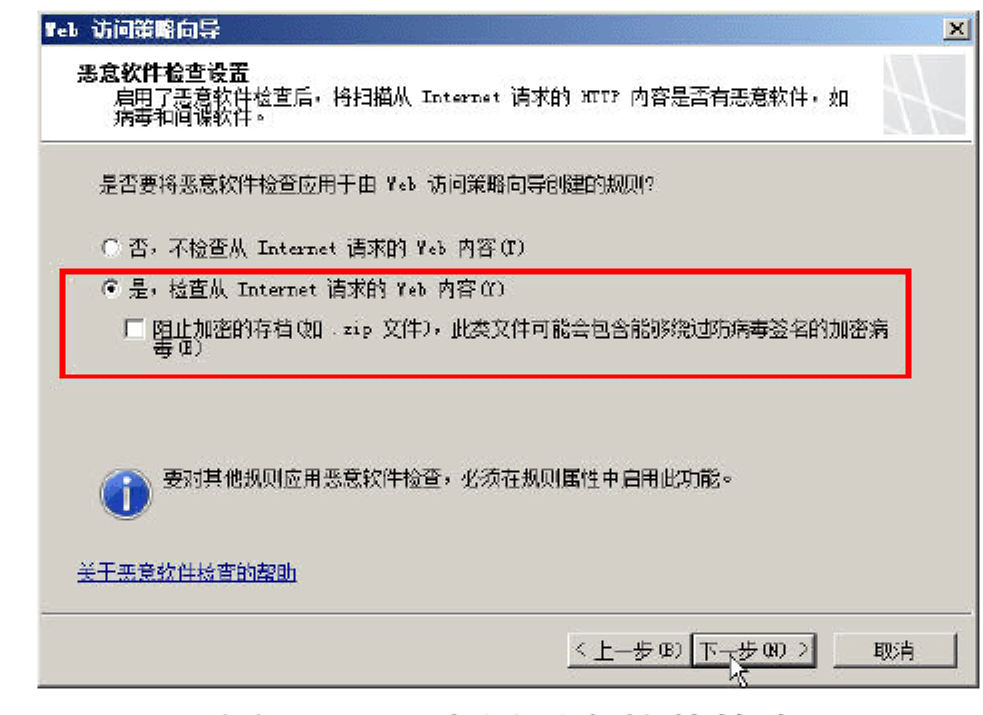


图 16-41　启用恶意软件检查

05 在“HTTPS 检查设置”对话框中，选择是否扫描 HTTPS 通信。一般情况下，不要检查 HTTPS 通信，且不验证 HTTPS 站点证书。如图 16-42 所示。

06 在“Web 缓存配置”对话框中，选择是否启用 Web 缓存规则，如果要启用缓存规则，须单击“缓存驱动器”按钮，设置缓存的磁盘及缓存大小，如图 16-43 所示。

07 在“正在完成 Web 访问策略向导”对话框中，单击“完成”按钮，如图 16-44 所示，Web 访问策略向导完成。

08 返回到 Forefront TMG 管理控制台后，单击“应用”按钮，让设置生效。如果在图 16-45 中启用了缓存，则会弹出“Forefront TMG 警告”对话框，在此选中“保存更改，并重启动服务”单选按钮；如果没有更改 TMG 的缓存，则不会出现该警告对话框。

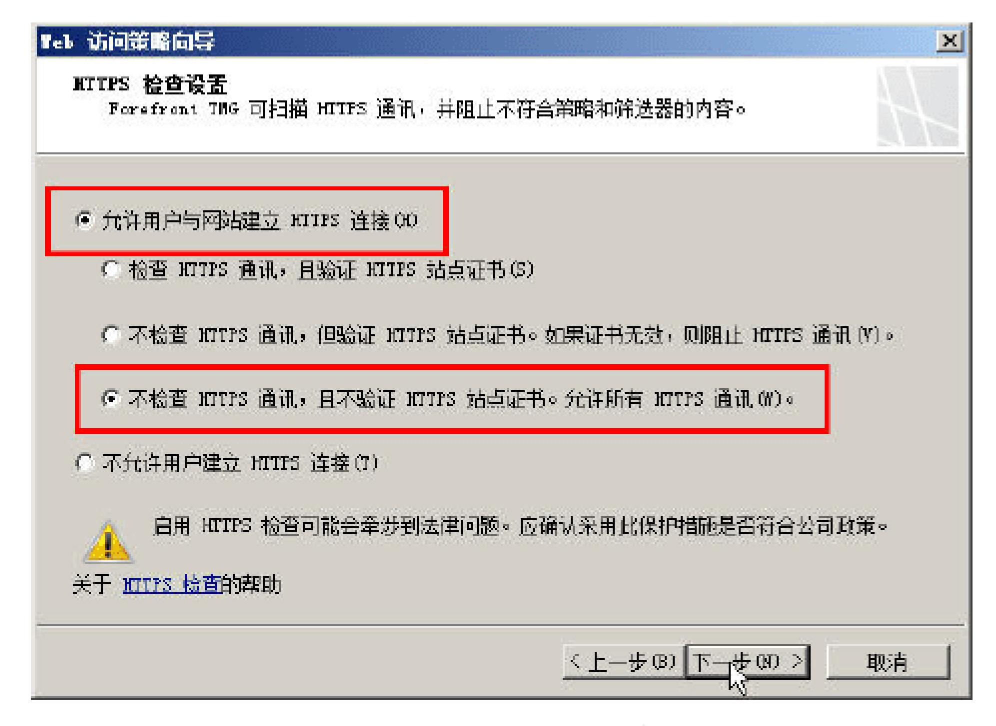


图 16-42　HTTS 扫描设置

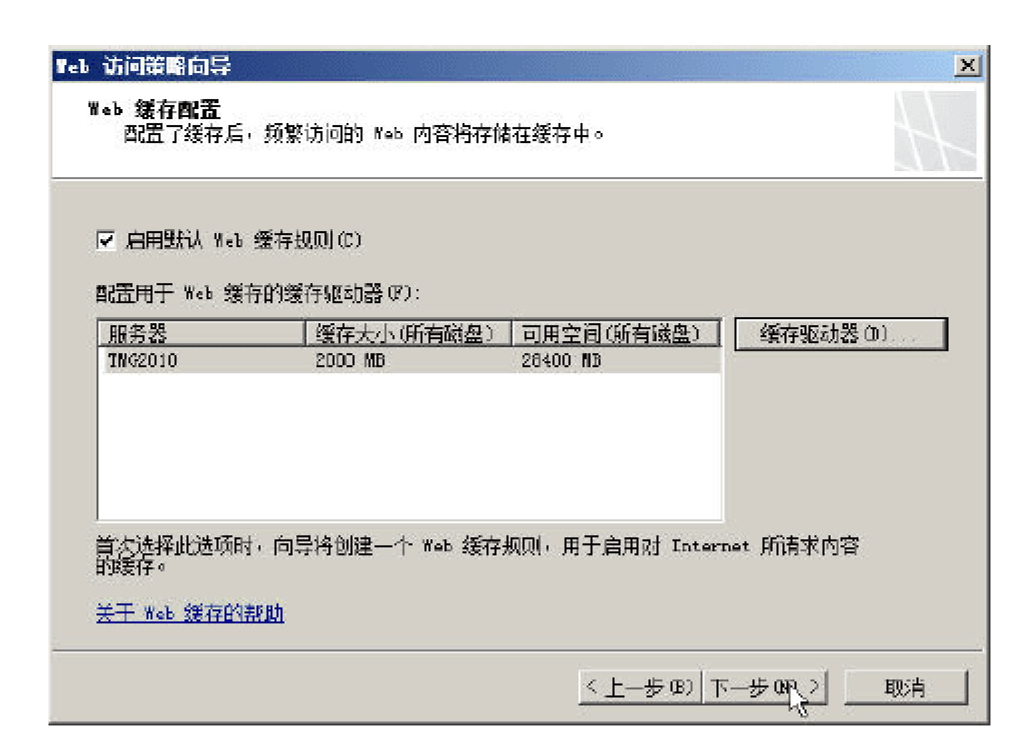


图 16-43　Web 缓存设置

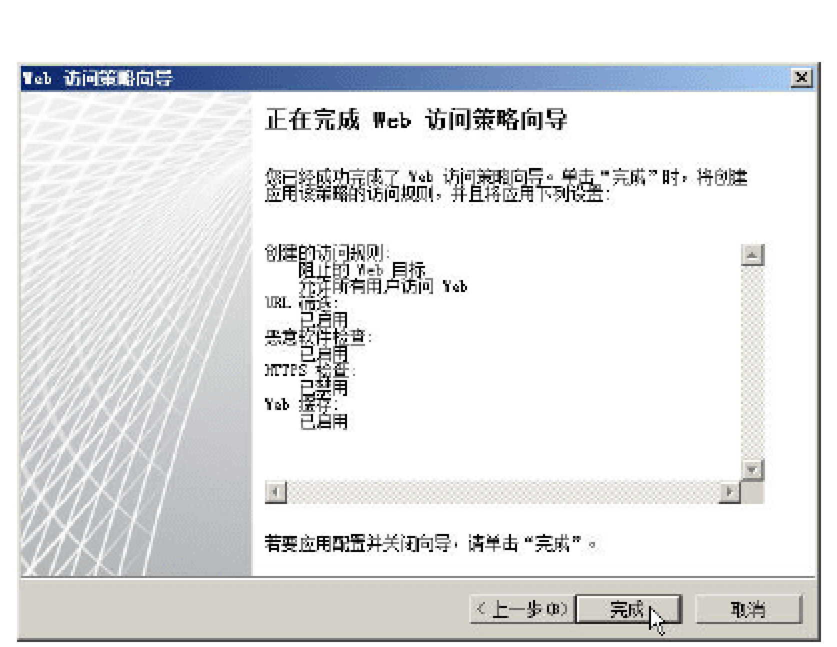


图 16-44　Web 访问策略向导完成

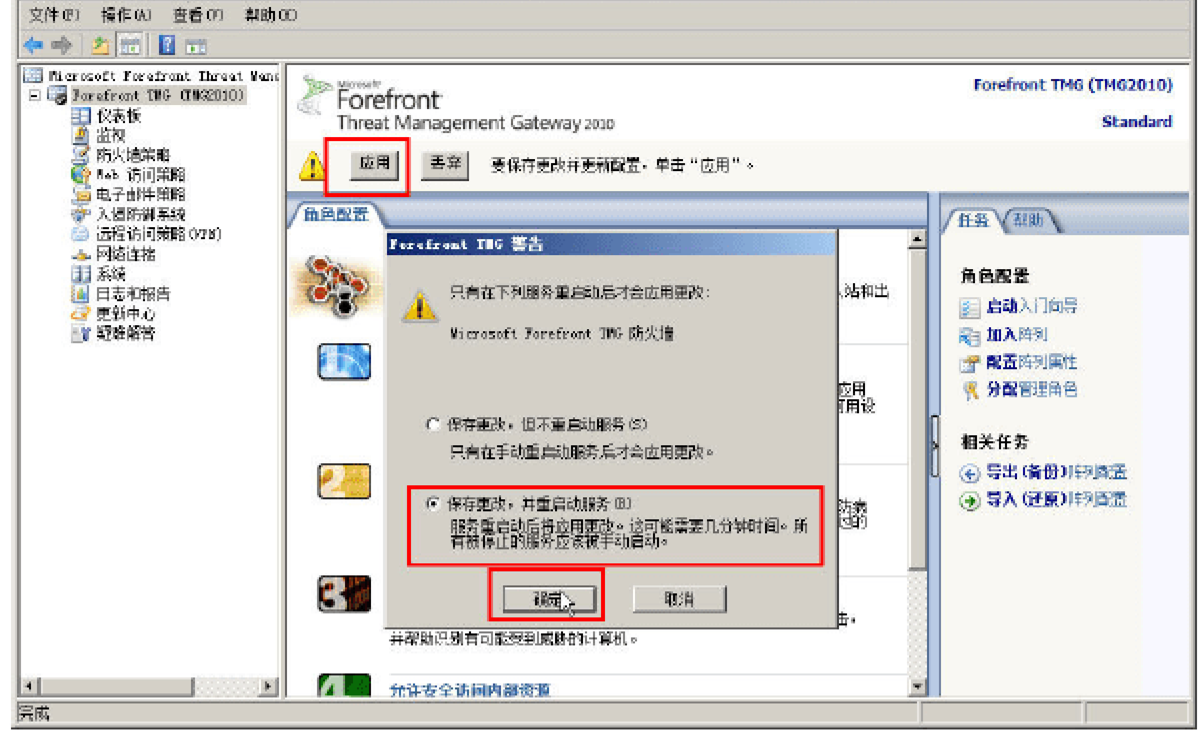


图 16-45　保存配置让设置生效

09 在 Forefront TMG 中，新增加了“配置更改描述”选项，每次更改配置之前，会弹出“配置更改描述”对话框，可以在“更改描述”文本框中写明更改 TMG 的原因与情况，以备以后检查，如图 16-46 所示；如果不需要出现该对话框，可选中“不再显示此提示”复选框。

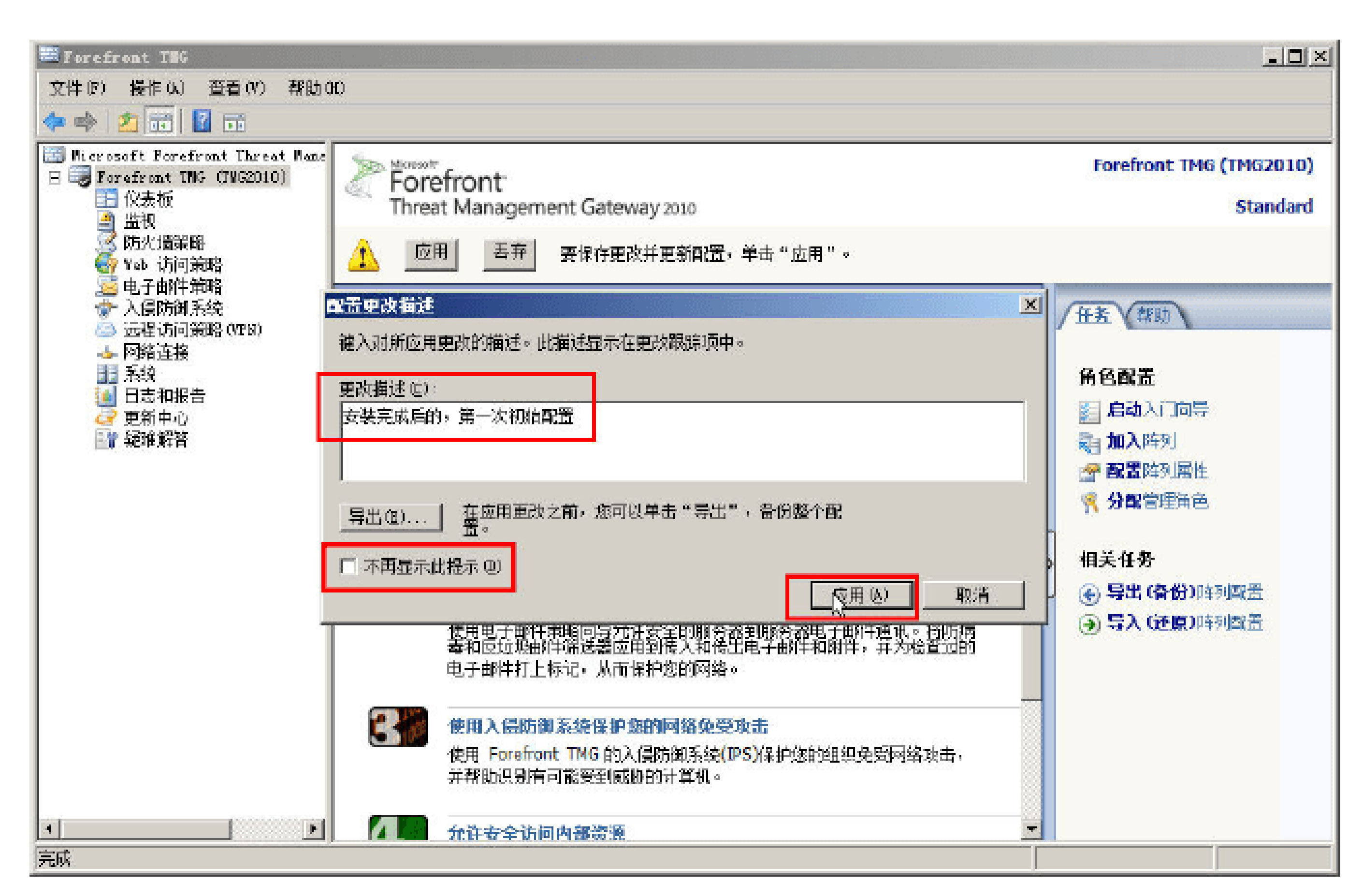


图 16-46　配置更改描述

此时，局域网中的其他计算机，就可以通过 Forefront TMG 正常上网。接下来，介绍 Forefront TMG 更加详细的配置。

16.3.5 Forefront TMG 控制台界面

为了让大家对 Forefront TMG 有一个总体的认识，本文简单介绍 Forefront TMG 的控制台界面。Microsoft Forefront Threat Management 2010 的控制台界面如图 16-47 所示。

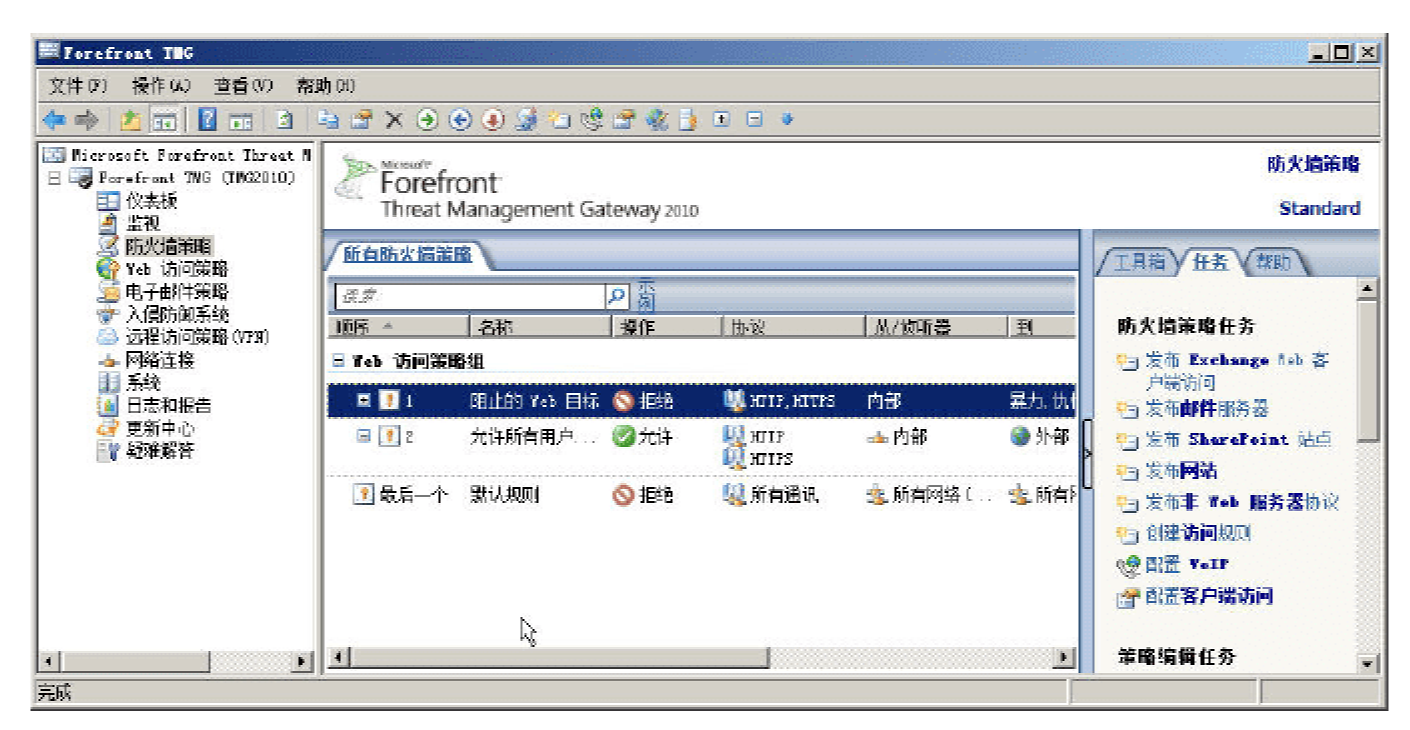


图 16-47　Forefront TMG 控制台界面

Forefront TMG 分左、中、右侧 3 个窗格，在左侧窗格中，显示了各个功能的选项，这包括“仪表板、监视、防火墙策略、Web 访问策略、电子邮件策略、入侵防御系统、远程访问策略（VPN）、网络连接、系统、日志和报告、更新中心、疑难解答” 12 大部分；在中侧窗格，包括两个部分，其中左边部分显示了每项的具体内容，右边部分显示了当前项的主要操作、任务等；而右侧窗格，默认没有显示，主要显示“操作”等内容，在 Forefront TMG 中，用处不大。在任何时候，都可以通过 Forefront TMG“工具栏”上的“ ”或“ ”按钮打开（显示）或关闭（隐藏）左侧或右侧窗格。另外，如果网络中有多台 Forefront TMG 服务器并且加入到同一阵列中，可以在左侧窗格中“Microsoft Forefront Threat Management Gateway”下面显示。在本例中，只有 1 台 Forefront TMG，所以会显示“Forefront TMG（TMG2010）”，其中 Forefront TMG 是当前的计算机名称。

16.4 防火墙策略

在 Forefront TMG 的“防火墙策略”中，可以通过定义防火墙规则，允许或拒绝对所连接网络、网站和服务器的访问，从而保护网络。总体来说，在“防火墙策略”中，创建的规则主要分为三种：

- 访问规则：允许从“源网络:（通常为本地主机、内部）”到“目的网络（通常为外部、外围、内部、本地主机”的访问。通常情况下，在访问规则中创建的都是出站访问，即从内部计算机到 Internet 的访问。
- Web 发布规则：控制对已发布的 Web 服务器的入站访问。
- 服务器发布规则：控制对已发布的非 Web 服务器的入站访问。

另外，与“防火墙策略”相对应的，还有 Forefront TMG 的“系统策略”。所谓系统策略，是控制进出“本地主机网络（Forefront TMG 服务器）”的通信，以允许 Forefront TMG 通过必需的通信和协议执行身份验证、享有域成员身份、执行网络诊断、日志记录和远程管理。



说　明

有关 Forefront TMG 的防火墙策略所需要的基础知识，可参见 “16.2 Forefront TMG 基础知识”一节内容。

16.4.1　防火墙策略基础

在创建或配置防火墙策略后，可以在 Forefront TMG 的“防火墙策略→所有防火墙策略”中，显示已经创建的防火墙策略与规则，如图 16-48 所示。

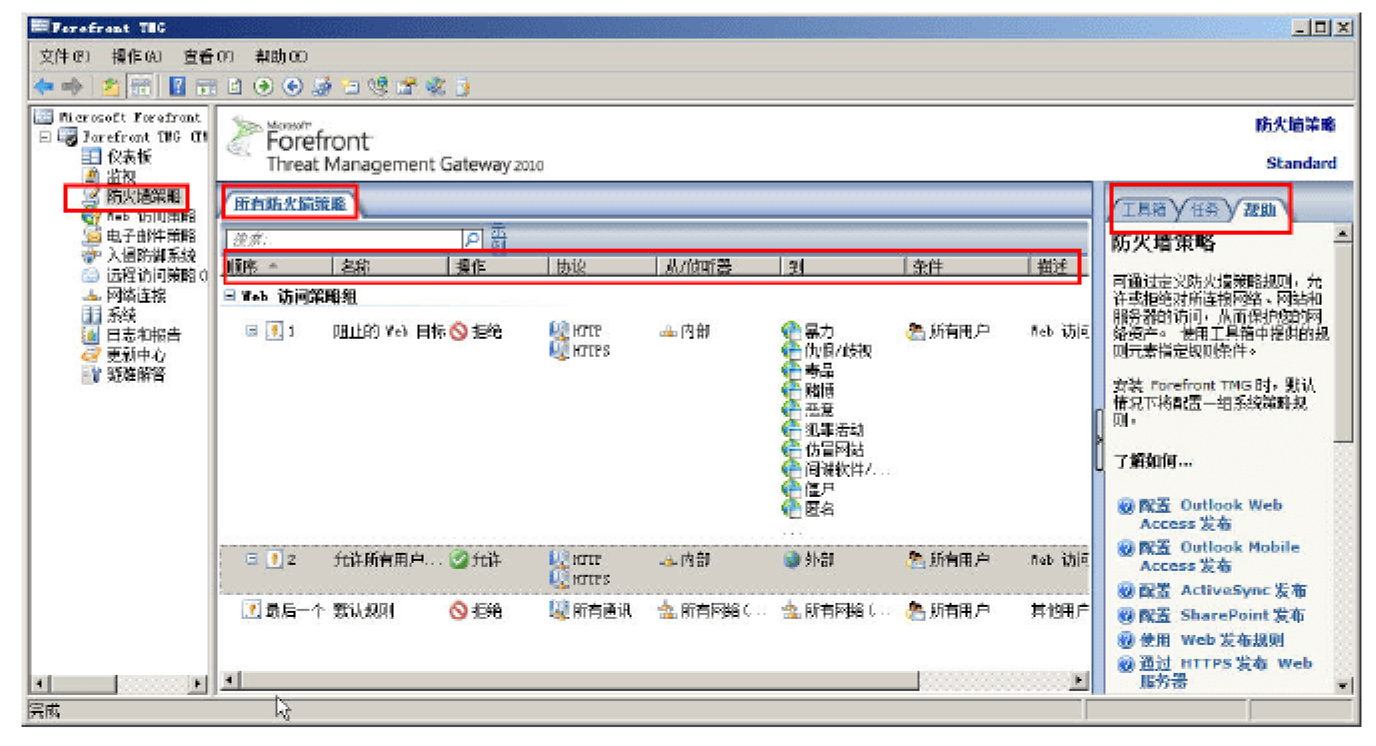


图 16-48　防火墙策略

在图 16-48 中，显示的访问规则是在运行 Forefront TMG 的入门向导时创建的，这些规则如下：

（1）第 1 条策略，策略的名称是“阻止的 Web 目标”，作用是“拒绝”“内部”网络“所有用户”到“暴力、仇恨/歧视、毒品、赌博、恶意、犯罪活动、仿冒网站、间谍软件、僵尸、匿名”这些网站的 Web 访问。

（2）第 2 条策略，策略的名称是“允许所有用户访问 Web”，作用是“允许”“内部”网络“所有用户”到“外部”所有网站的 Web 访问。

要学会或精通 Forefront TMG，必须要理解策略的意义，这些包括：

（1）每条策略，包括顺序、名称、操作、协议、从、到、用户、计划、内容类型等项。如果是 Web 访问策略，还会包括“恶意软件检查”项。在 Forefront TMG 的“防火墙策略”中，用鼠标双击一条已经创建的策略，可以看到这些项，如图 16-49 所示。

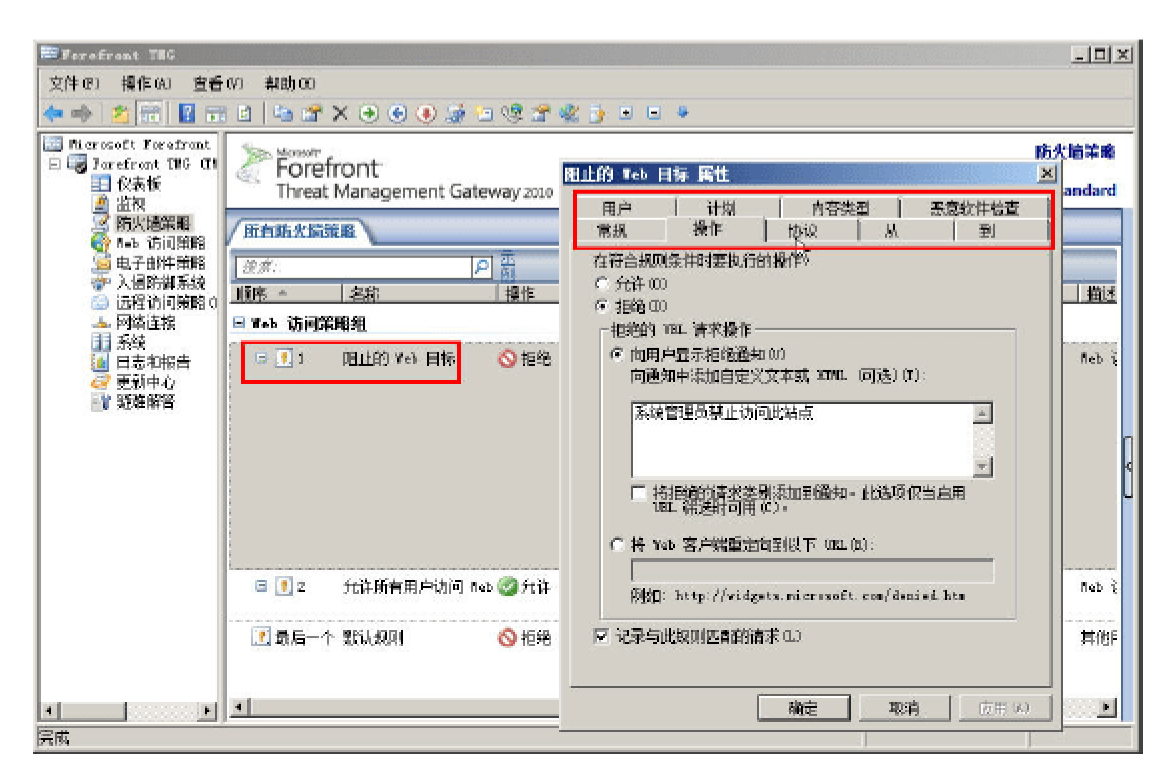
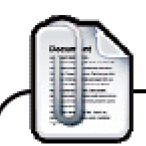


图 16-49　策略

（2）策略匹配。所谓策略的匹配，要符合策略中除“常规（包括策略的名称、描述项等）”、“操作”以外的所有条件（协议、从、到、用户、计划、内容类型）全部同时满足时，才叫策略匹配。



说 明

在 Forefront TMG 的策略中，“计划”指的是时间对象。在 Forefront TMG 所保护（控制）的网络中，计划的时间是以 Forefront TMG 计算机为基准，并不以用户的时间为准。如果 Forefront TMG 加入到 Active Directory 中，则以 Active Directory 中第一台域控制器的时间为准。

（3）策略顺序。策略是有顺序的，并且从上到下（根据序号，从小到大）进行查找匹配，并且，在找到第一条匹配的策略时，根据“策略匹配”中指定的“操作（允许或拒绝）”进行控制，Forefront TMG 将不再向下查找。如果查找完所有策略，找不到相匹配的策略时，Forefront TMG 将会“拒绝”这种行为。

例如，在上面的两条策略中，如果将“允许所有用户访问 Web”策略移到“阻止的 Web 目标”策略前，那么，所有用户将能够访问所有的网站，包括“暴力、仇恨/歧视、毒品、赌博、恶意、犯罪活动、仿冒网站、间谍软件、僵尸、匿名”这些网站，这样就与我们的规则不相符合了。

（4）可以改变策略顺序。Forefront TMG 中的策略顺序并不是一成不变的，管理员可以根据需要，选择其中的一条或多条策略，通过单击工具栏上的“↑”或“↓”按钮进行向上或向下的调整。

（5）可以启用或停用策略。管理员可以根据需要，停用某条或多条策略；并且可以根据需要，再次启用这些或某条策略。

（6）对于不需要的策略，可以根据需要删除。策略也可以复制、粘贴、修改。在 Forefront TMG 中，可以将多条策略进行“组合”以及“取消组合”。

在理解了 Forefront TMG 策略的意义后，就可以更容易地根据企业的需求，创建适合自己的策略。接下来将介绍在 Forefront TMG 中，访问规则的创建、修改、删除、组合等内容。

16.4.2 通过案例介绍访问规则与服务器发布规则

在使用 Forefront TMG 创建访问规则之前，需要对 Forefront TMG 保护的网络进行规划，并且根据规划的内容按照顺序创建规则。

事实表明，没有任何两个网络会完全一致。同样，即使网络拓扑完全相同的网络，其网络规则也不会完全一致。但是，对于初学者来说，参考他人的规则，并且根据自己所管理的网络进行适当的调整，是最快掌握 Forefront TMG 的方法。在本节中，将通过一个具体的案例，介绍网络的规划与防火墙策略的创建。

在图 16-50 中，Forefront TMG 保护的网络划分为 12 个 VLAN，其中 VLAN11（IP 地址段为 192.168.1.0/24）、VLAN12（IP 地址段为 192.168.2.0/24）并依次类推，直到 VLAN20（IP 地址段为 192.168.10.0/24）这 10 个网段，被工作站使用；VLAN100（IP 地址段为 192.168.100.0/24）被服务器所使用；VLAN200（IP 地址段为 192.168.254.0/24）被 TMG2010 服务器“内网网卡”所使用。

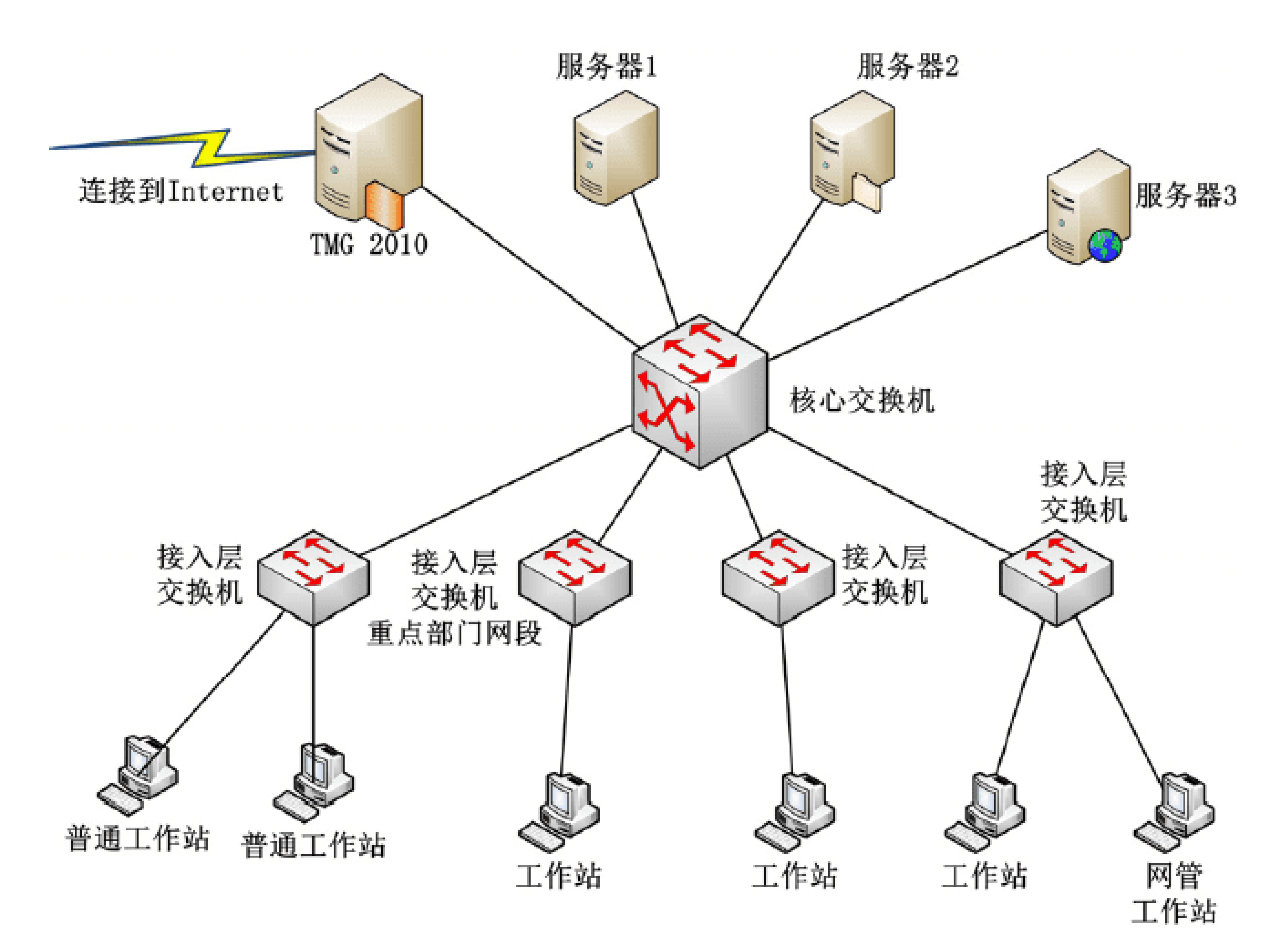


图 16-50　网络示例

在这些网段中，需要注意的是：

- VLAN100 是服务器工作的网段，其中服务器 1、服务器 2（IP 地址分别是 192.168.100.10 与 192.168.100.11）分别是电子邮件服务器、杀毒软件与 WSUS 升级服务器，这两台服务器需要能够访问 Internet；服务器 3（IP 地址是 192.168.100.20）是网站与 FTP 服务器，供内网用户访问，同时也将这个网站发布到 Internet，供 Internet 用户访问，但服务器 3 不需要访问 Internet。
- VLAN16 网段是重点部门网段，安全性要高。只允许周一到周五的每天上午 8:00~11:00 上网，在上网时段不允许以 FTP 协议向外上传文件；其他时间不允许上网。
- VLAN18 网段是领导等部门网段，在任何时间都不要进行限制。
- 其他网段（VLAN11 ~ VLAN15、VLAN17、VLAN19、VLAN20），在周一到周五的上午 8:00 ~ 12:00、下午 14:00 ~ 17:00，只允许访问网站、收发邮件。在此之外的其他时间，则不做限制。

基于上述这些要求，我们规划的策略如下：

（1）创建访问规则 1：允许 VLAN18（192.168.8.0/24）以“所有协议”访问“外部”。

（2）创建访问规则 2：允许 VLAN16（192.168.6.0/24）以“HTTP、FTP 协议”在周一到周五的上午 8:00～11:00 访问“外部”。

（3）创建访问规则 3：允许服务器 1（192.168.100.10）以“HTTP 协议、POP3、SMTP 协议”访问“外部”。

- 创建服务器发布规则 1：发布电子邮件服务器到 192.168.100.10。
- 创建服务器发布规则 2：发布 Web 服务器到 192.168.100.10，域名为 mail.msft.com（假设该邮件服务器对外提供的域名是 mail.msft.com）。

（4）创建访问规则 4：允许服务器 2（192.168.100.11）以“HTTP 协议”访问“外部”。

（5）创建访问规则 5：拒绝服务器 3（192.168.100.20）以“任何协议”访问“外部”。

- 创建服务器发布规则 3：发布 Web 服务器到 192.168.100.20，域名为 www.msft.com。
- 创建服务器发布规则 4：发布 FTP 服务器到 192.168.100.20。

（6）创建访问规则 6：允许其他网段在周一到周五的 8:00～11:00、14:00～17:00，以“HTTP、FTP、SMTP 与 POP3 协议”访问“外部”，在其他时间以“所有协议”访问“外部”。

1. 访问规则 1 的创建

接下来，我们创建访问规则。在创建访问规则之前，先检查 Forefront TMG 已经创建的访问策略（参看图 16-48），在运行 Forefront TMG 的 Web 访问向导之后，创建了两条策略：其中第 1 条是“阻止的 Web 目标”，这条策略的目的是拒绝“内部”到“暴力、仇恨”等这些站点的访问。另 1 条是“允许所有用户访问 Web”，这条策略的目的是允许“内部”到“外部”以 HTTP 协议与 HTTPS 协议访问。那么，我们在创建访问规则时，如果不想使用这些策略，可以删除或停用这 2 条策略。或者，可根据需要，修改保留其中的策略。在本例中，我们保留第 1 条策略（阻止的 Web 目标），并且将这条策略保持在所有策略的前面。而在当前的第 2 条策略与第 1 条策略之间，插入我们新创建的策略。我们首先介绍前文规划的访问规则 1 的创建步骤。

01 在 Forefront TMG 的“防火墙策略”中，先用鼠标选中第 2 条策略，然后用鼠标右击“防火墙策略”，在弹出的快捷菜单中选择 “新建→访问规则”，如图 16-51 所示。这时创建的访问规则将会“插在”当前第 1、2 条策略之后。以后创建策略的时候，如果是插在当前策略之后，应该是选中当前策略之后的下一条策略，然后再次选择创建。

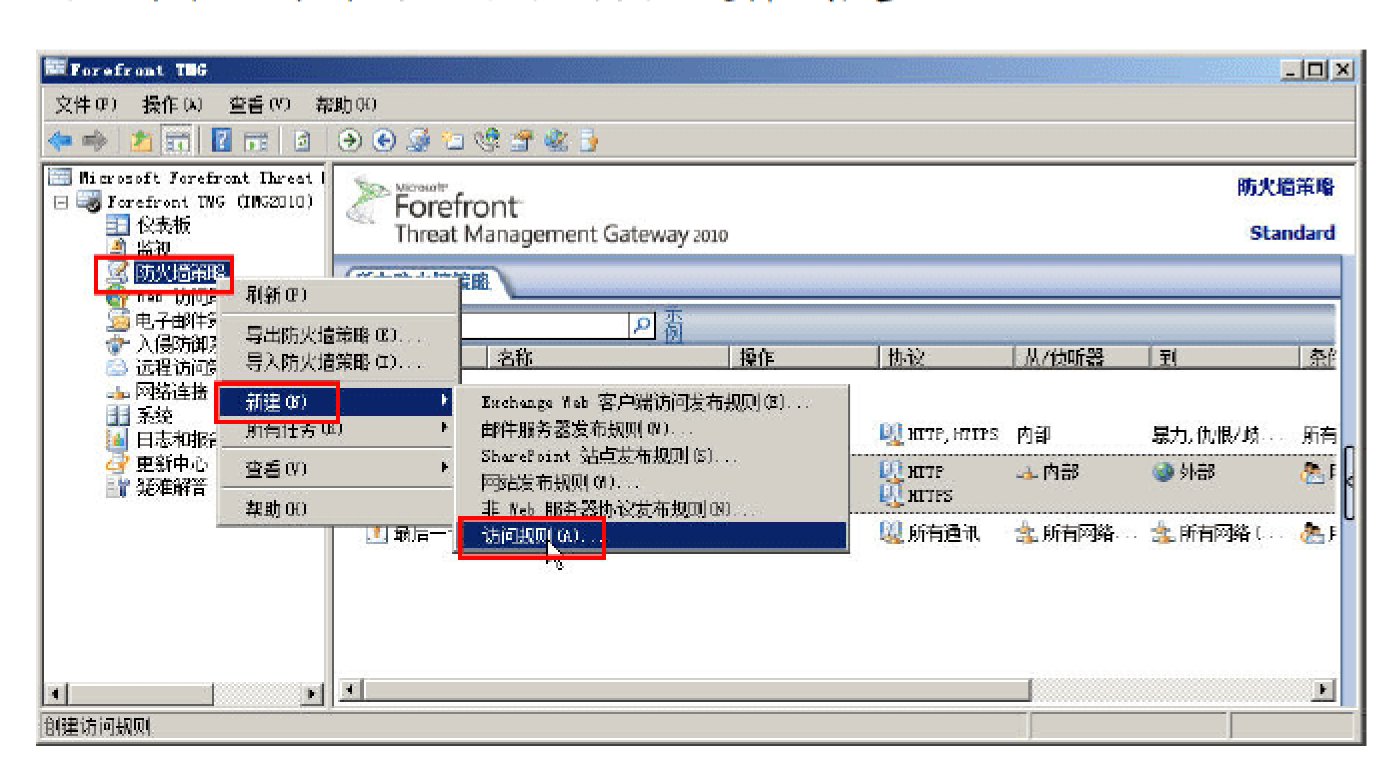


图 16-51 创建访问规则

02 在“欢迎使用新建访问规则向导”对话框中，在“访问规则名称”文本框中，输入当前创建的规则的名称，在此设置为“允许 VLAN18 访问外部”，如图 16-52 所示。当然，也可以设置其他有意义的名称。

03 在“规则操作”对话框中，选中“允许”单选按钮，如图 16-53 所示。

04 在“协议”对话框中，在“此规则应用到”下拉列表中，选择“所有出站通信”选项，如图 16-54 所示。

05 在“恶意软件检查”对话框中，选中“不对该规则启用恶意软件检查”单选按钮，如图 16-55 所示。

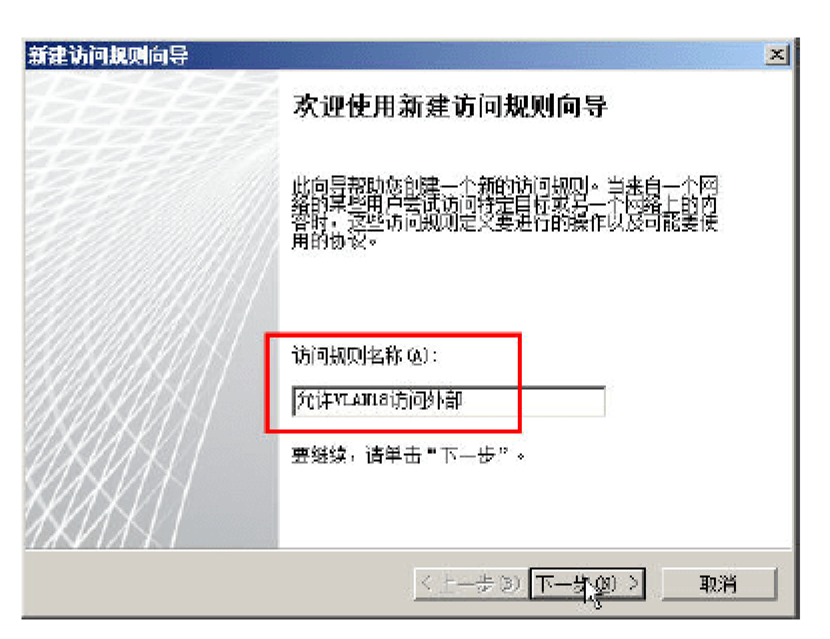


图 16-52　设置规则名称

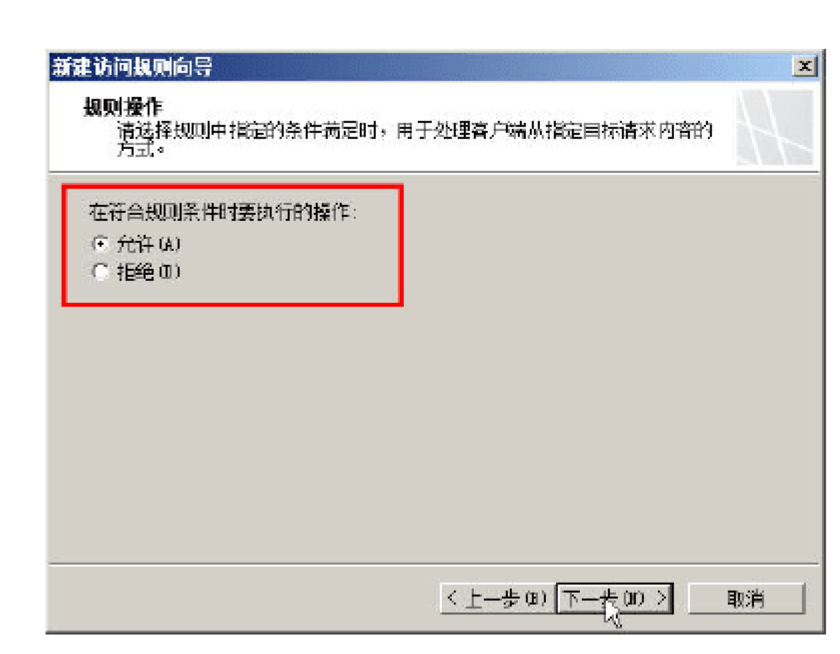


图 16-53　规则操作

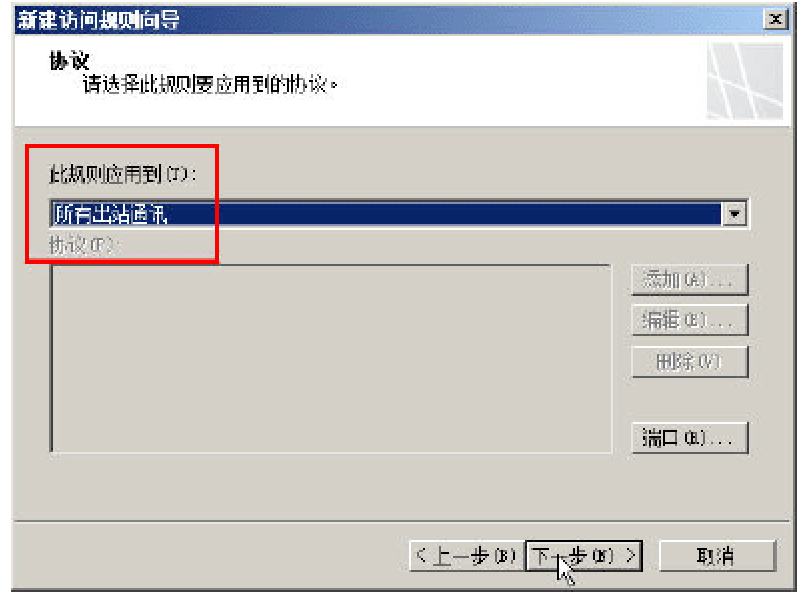


图 16-54　协议

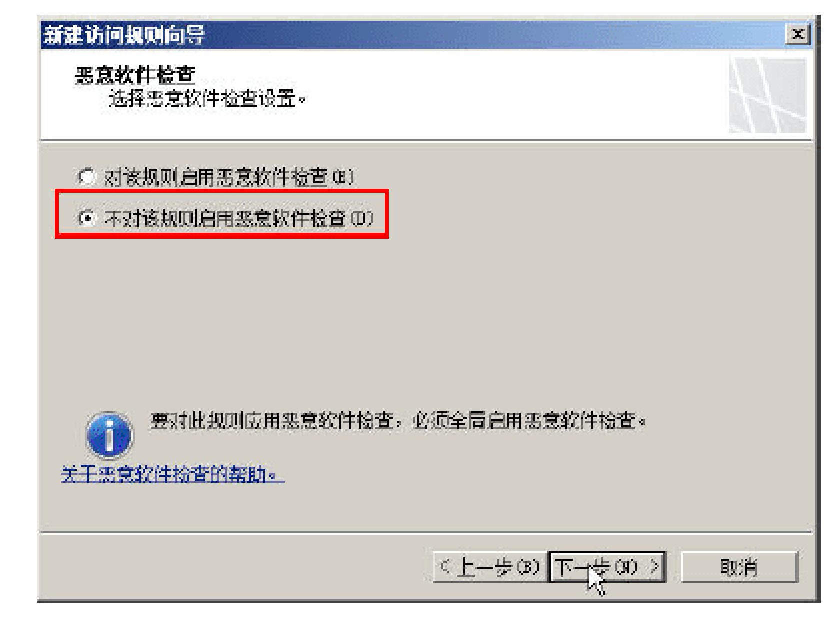


图 16-55　恶意软件检查

06 在“访问规则源”对话框中，选择源地址（网络或计算机），因为 VLAN18 所包含的地址范围，在 Forefront TMG 中没有定义，所以需要创建一个。在此对话框中，单击“添加”按钮，在弹出的“添加网络实体”对话框中，单击“新建”按钮，在弹出的菜单中选择“子网”命令，在弹出的“新建子网规则元素”对话框中，设置创建的网络规则名称，在本例中为 VLAN18，然后在“网络地址”文本框中输入创建的网络的地址，在本例中是 192.168.8.0，然后输入对应的子网掩码 255.255.255.0，也可以输入子网掩码位数（24 位），如图 16-56 所示。

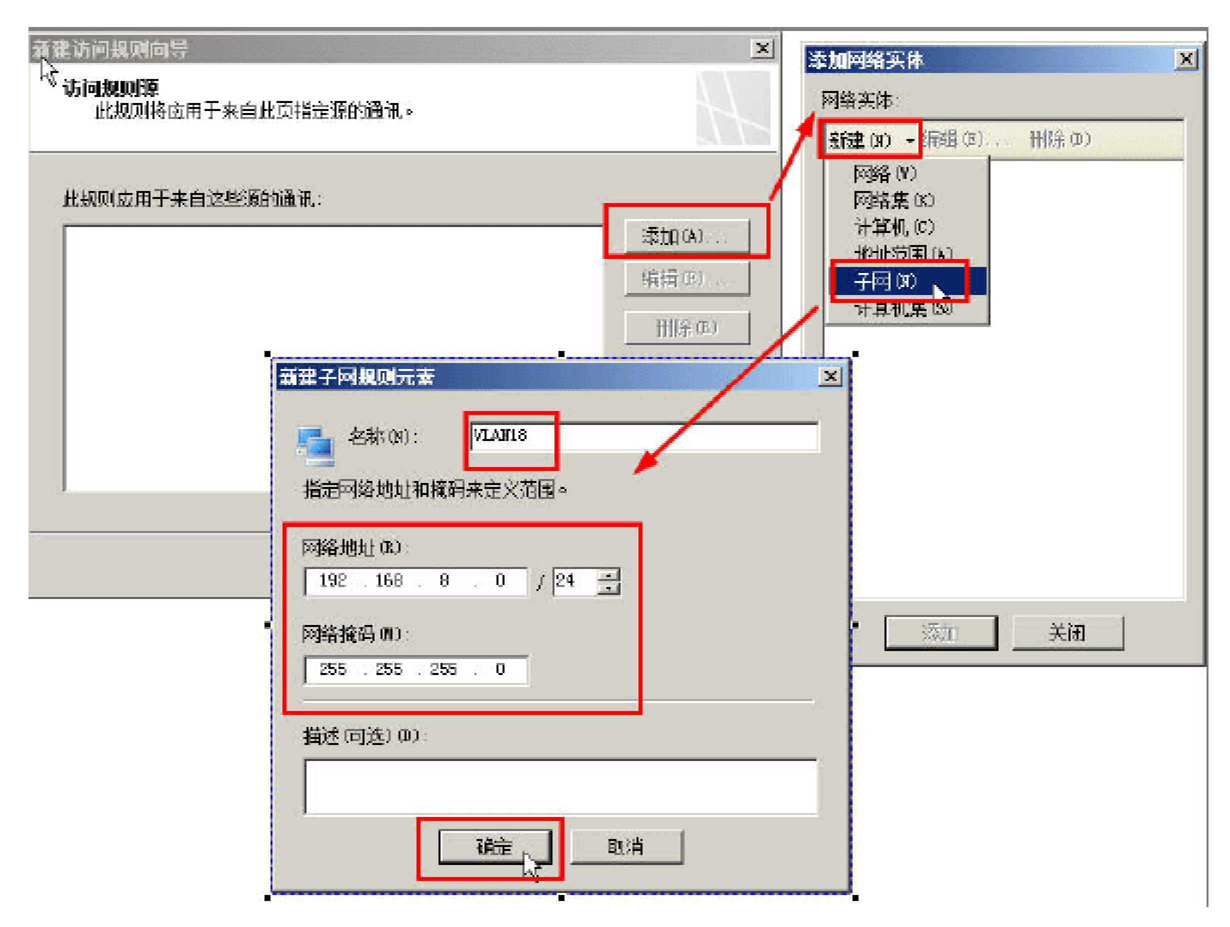


图 16-56　添加子网

创建完成后，单击“确定”按钮返回到“添加网络实体”对话框，然后在“子网”选中新创建的子网名称，单击“添加”按钮添加到“访问规则源”中，如图 16-57 所示。

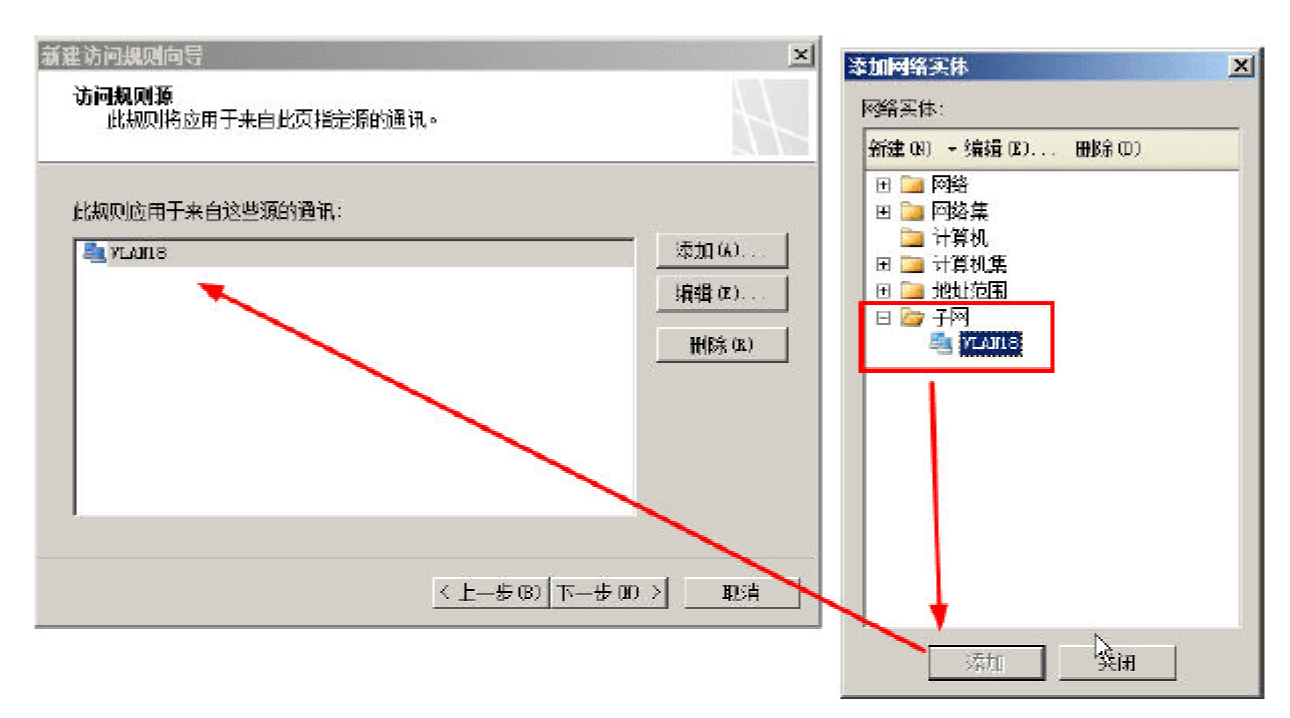


图 16-57　添加访问规则源



说 明

在“添加网络实体”中，可以创建多个实体，这些实体可以是一台计算机（一个 IP 地址），可以是一组计算机（一个网段或一段指定的 IP 地址），也可以是包括域名的计算机等，或者是这些的组合。另外，在“访问规则源”中，可以添加多个“源”。

07 在“访问规则目标”对话框中，单击“添加”按钮，在弹出的“添加网络实体”对话框中，从“网络”列表中选中“外部”进行添加，如图 16-58 所示。

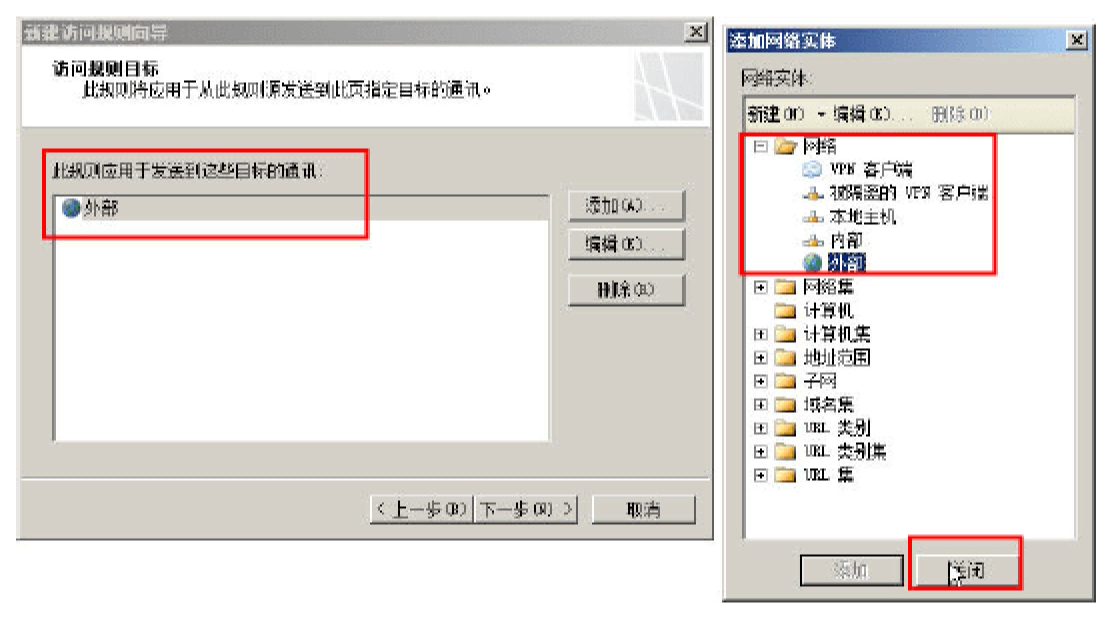
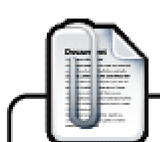


图 16-58　访问规则目标



说 明

在“访问规则目标”对话框中，可以添加多个实体。

08 在“用户集”对话框中，选择默认值，在此是“所有用户”，如图 16-59 所示。

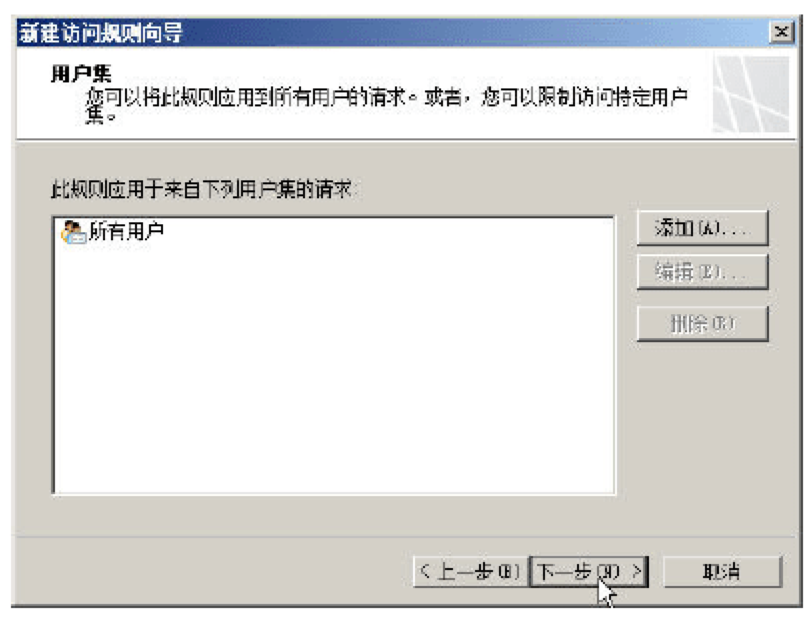
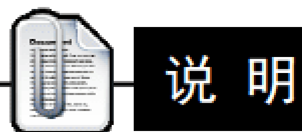


图 16-59　用户集



说 明

只有 Forefront TMG 和网络中的计算机都加入到 Active Directory，并且使用“防火墙客户端”时，此项才有实际意义。一般情况下，选择默认值“所有用户”即可。

09 在“正在完成新建访问规则向导”对话框中，单击“完成”按钮，完成规则的创建。

2. 访问规则 2 的创建

访问规则 2 的内容是：允许 VLAN16（192.168.6.0/24）以“HTTP、FTP 协议”在周一到周五的上午 8:00～11:00 访问“外部”。

访问规则 2 与访问规则 1 类似，只是多了一个“计划”时间范围：周一到周五的 8:00～11:00”。接下来介绍这个规则的创建。

01 定位到上次创建的规则的下一条规则，用鼠标右击“防火墙策略”，选择“新建→访问规则”命令，如图 16-60 所示。

02 设置访问规则名称为“VLAN16 访问规则”，如图 16-61 所示。

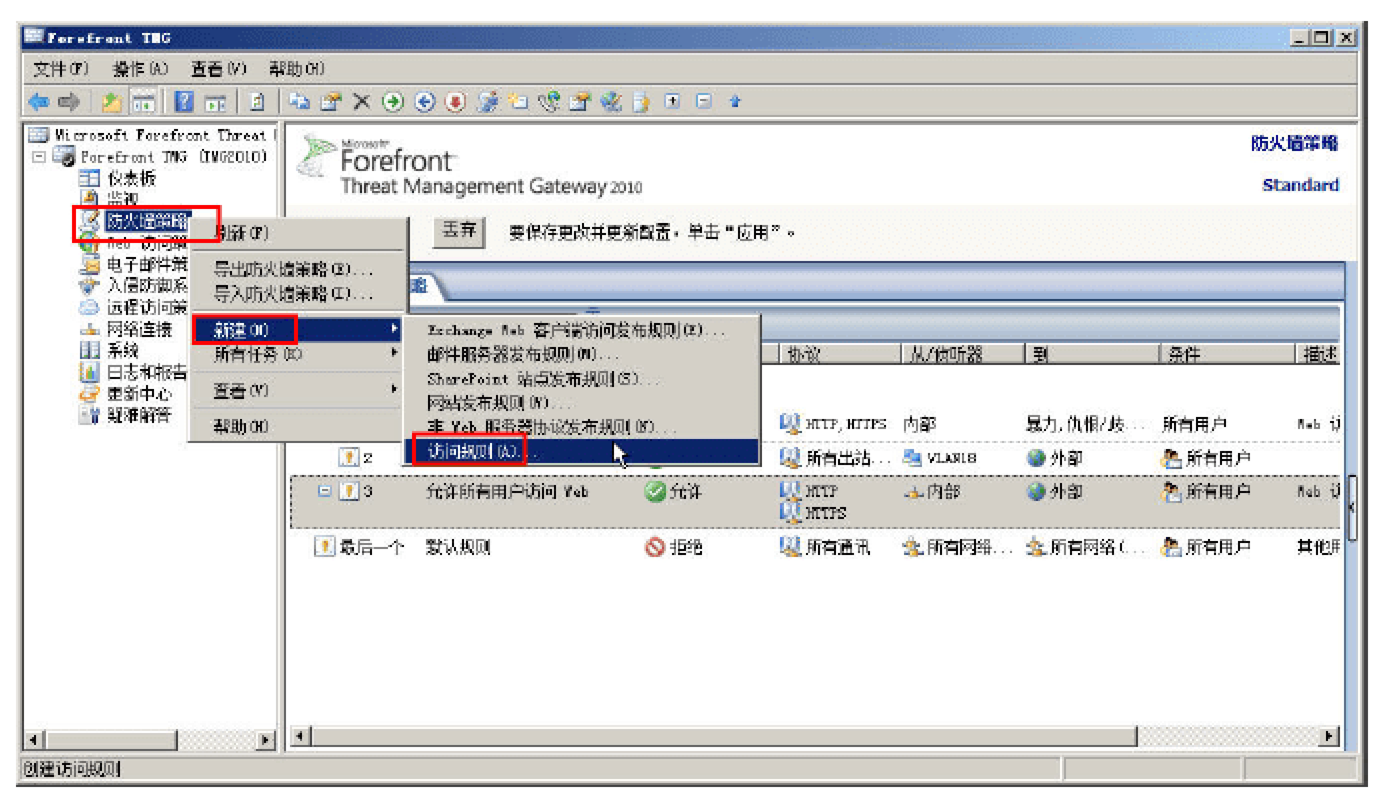


图 16-60　新建访问规则

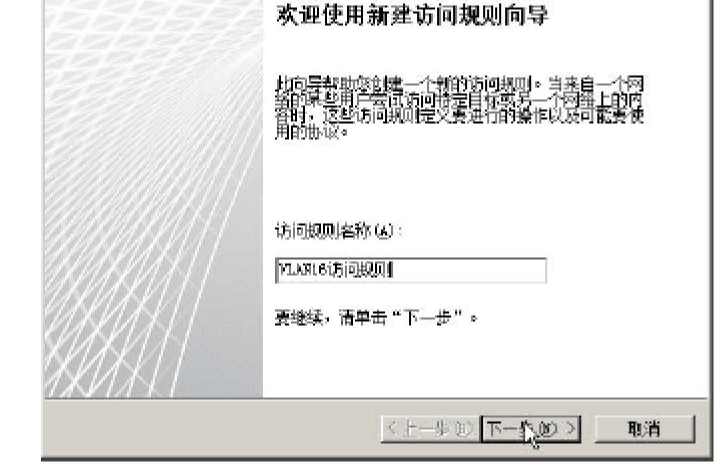


图 16-61　访问规则名称

03 在“规则操作”对话框中选择“允许”。

04 在“协议”对话框中，选择“FTP、HTTP、HTTPS”，如图 16-62 所示。

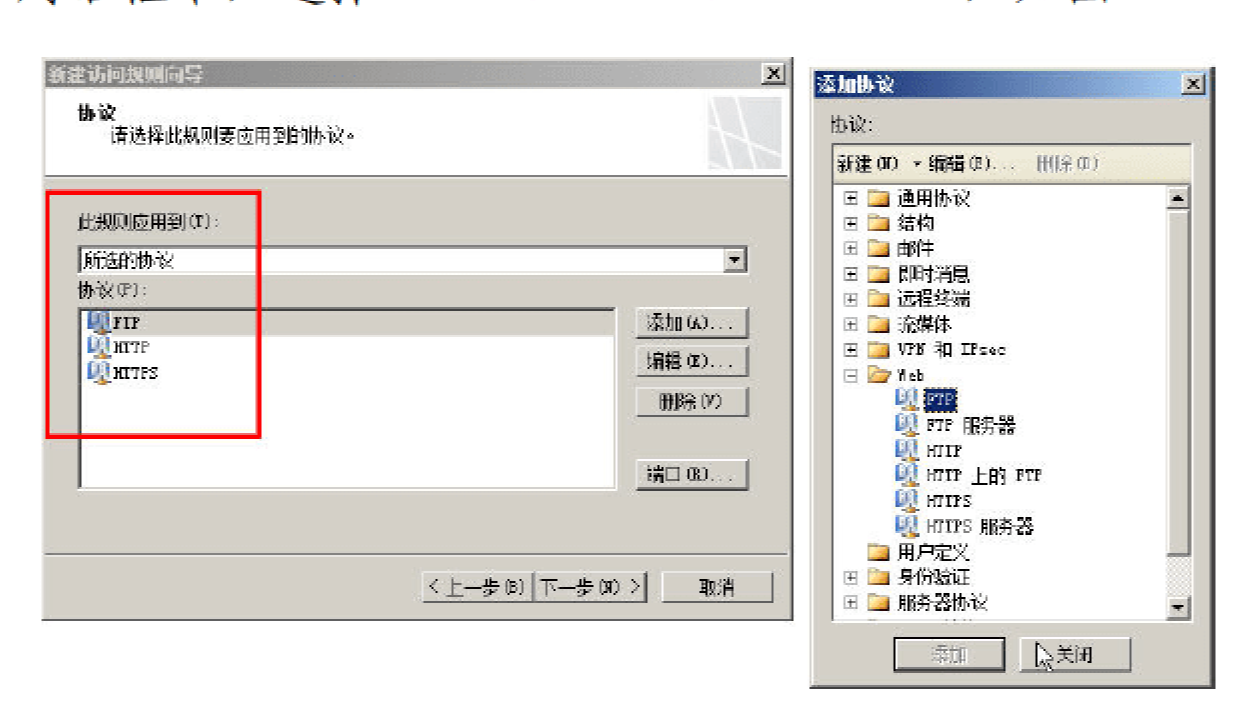


图 16-62　协议选择

05 在“访问规则源”对话框中，创建 VLAN16（IP 地址段为 192.168.6.0/24）的地址段，并

添加到访问规则源中，如图 16-63 所示。

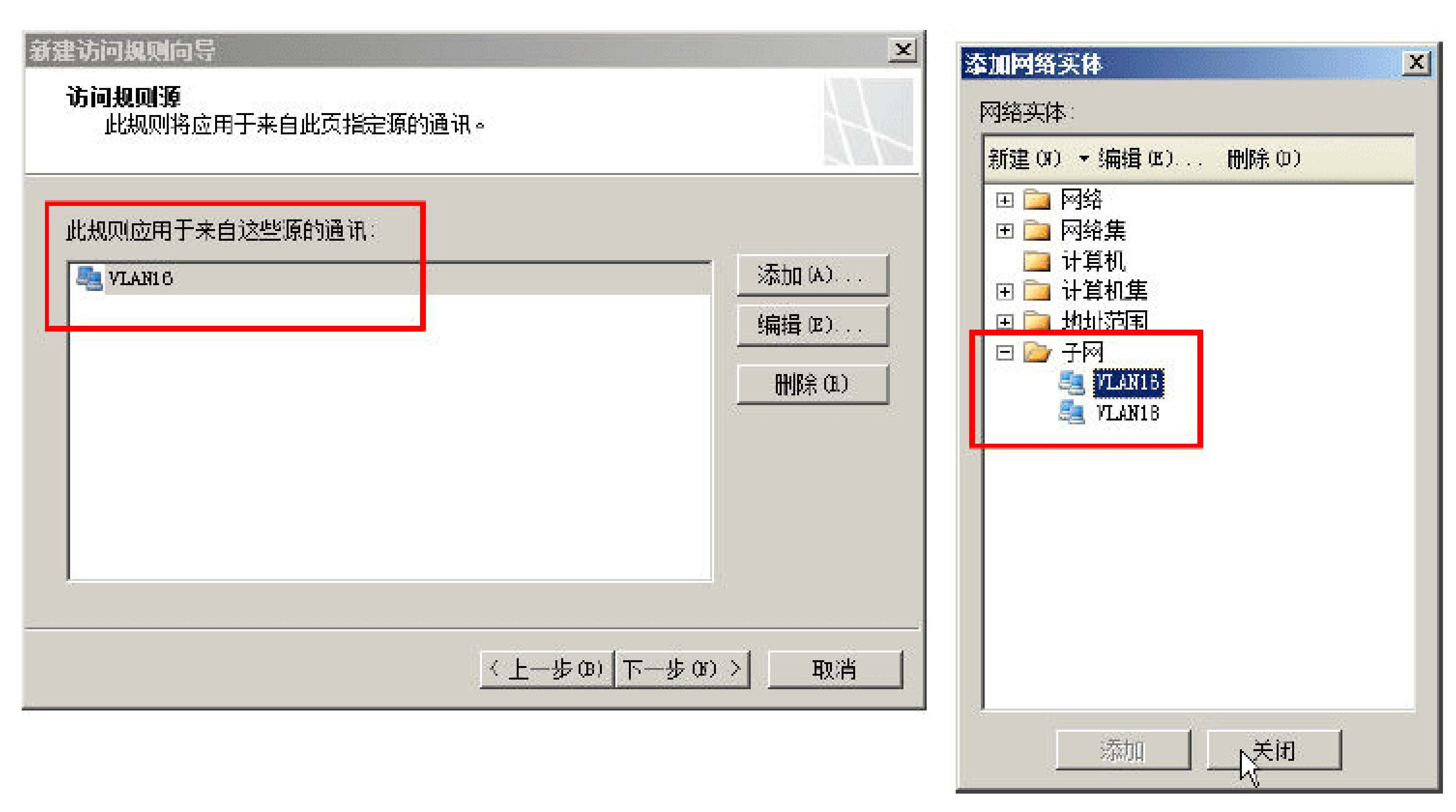


图 16-63 访问规则源

06 其他操作与访问规则 1 相同，不再介绍。

创建完“VLAN16 访问规则”后，返回到 Forefront TMG 控制台，然后用鼠标双击这条规则，进行下面的操作。

01 在“VLAN16 访问规则 属性”对话框中的“计划”选项卡中，可以看到默认计划的时间是“总是”，并且在图示中看到标明的是所有的时间。单击“新建”按钮，创建我们所规划的时间。在弹出的“新建计划”对话框中，设置名称为“周 1-5 上午 8-11 点”，然后选中星期一到星期五的 8:00 ~ 11:00 的范围为“活动”，如图 16-64 所示。

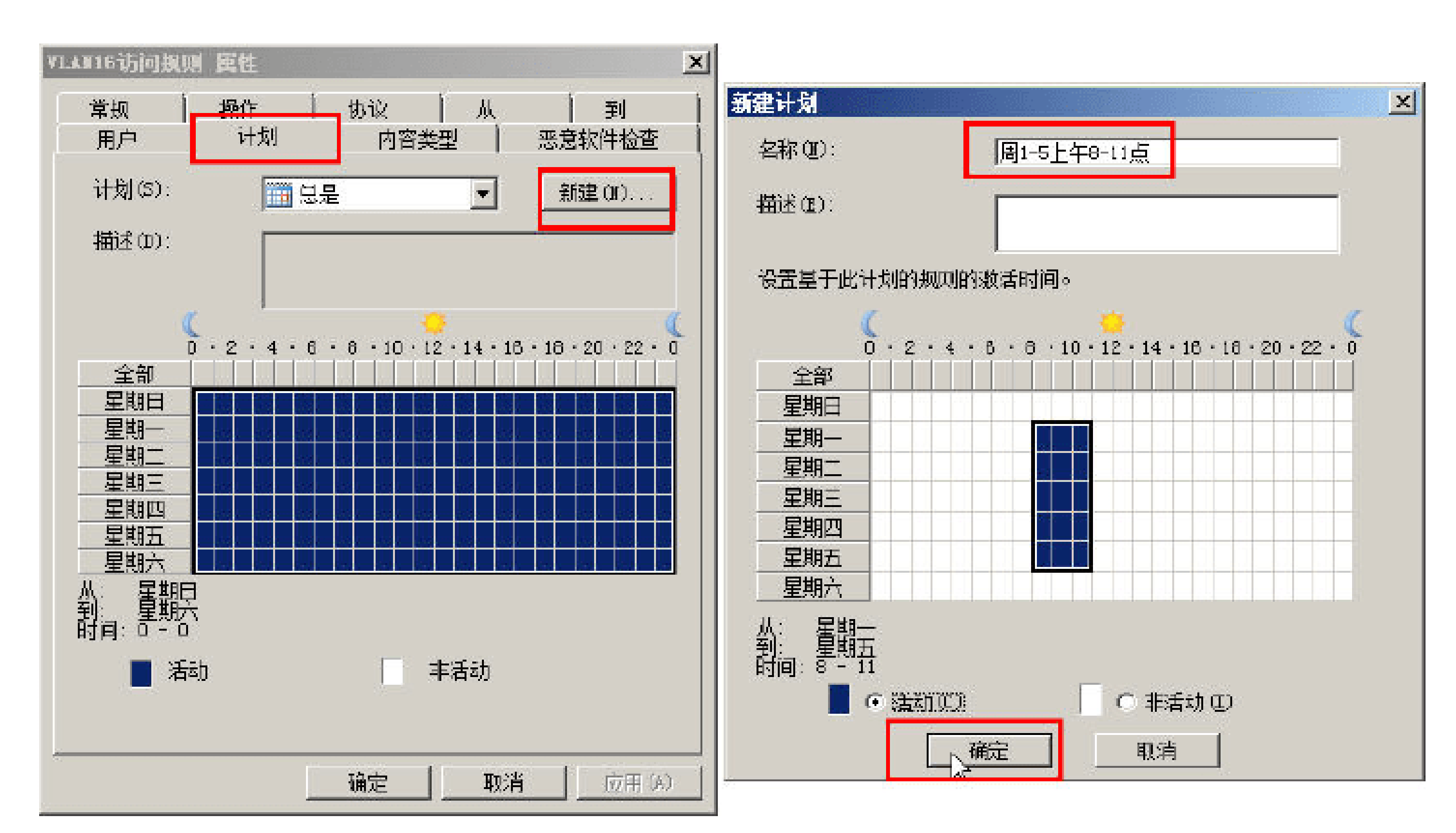


图 16-64 添加新计划

说 明

可以先单击“非活动”单选按钮以取消所有时间，然后用鼠标左键单击选中需要的时间段（按住鼠标左键移动选取），然后再单击“活动”单选按钮即可选中。

02 选中之后，在“计划”下拉列表中选择创建的“周 1-5 上午 8-11 点”，然后单击“确定”按钮即可，如图 16-65 所示。

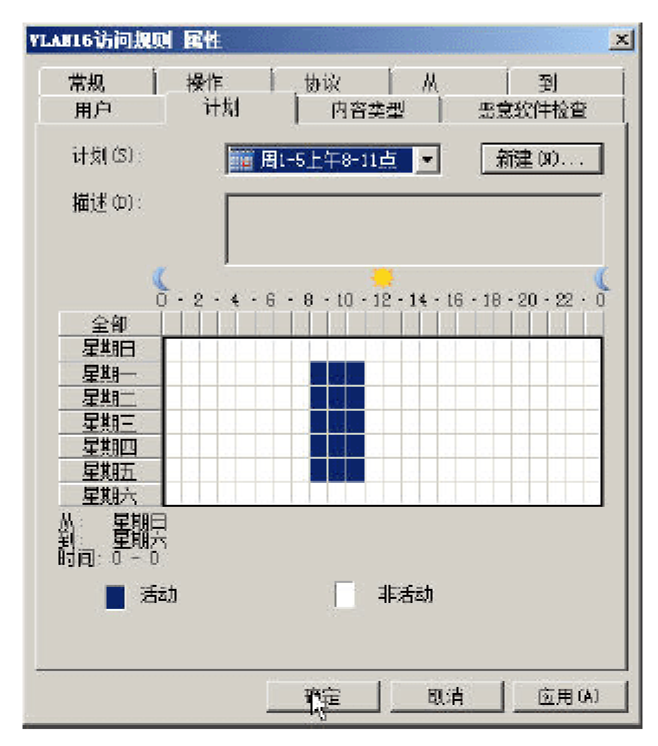


图 16-65　选择计划

3. 访问规则 3 的创建

创建访问规则 3“允许服务器 1（192.168.100.10）以 HTTP 协议、POP3、SMTP 协议访问外部”，这条规则的创建，与创建访问规则 1 非常类似，只有以下几点不同。

01 在“欢迎使用新建访问规则向导”对话框中，设置访问规则名称为“允许服务器 1 以 HTTP、POP3、SMTP 协议访问外部”，如图 16-66 所示。

02 在“协议”对话框中，选中“HTTP、POP3、SMTP”，如图 16-67 所示。

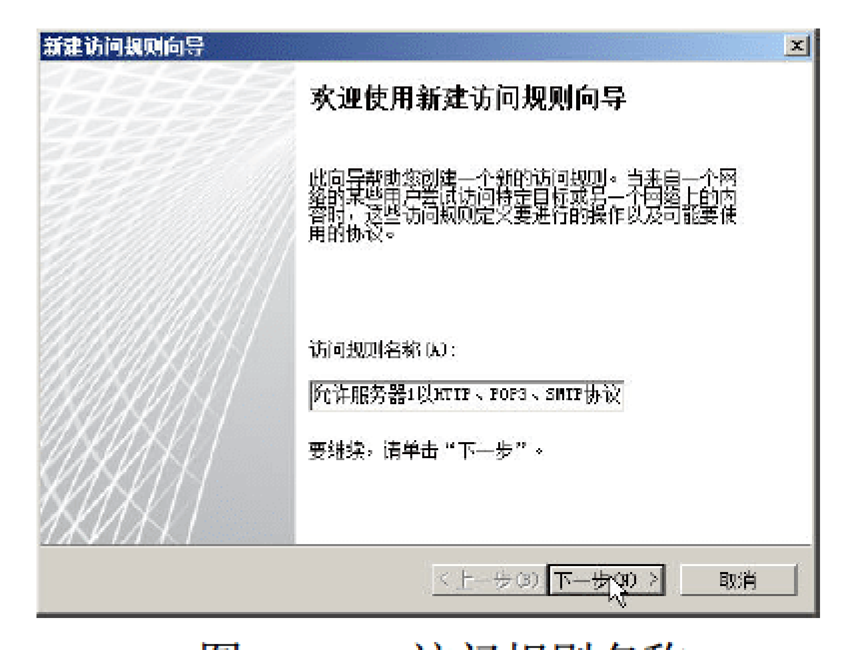


图 16-66　访问规则名称

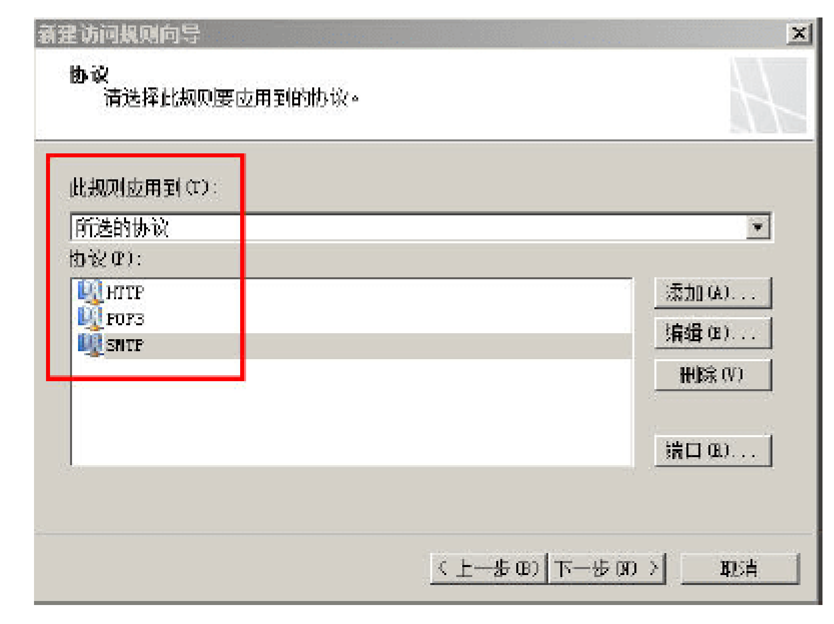


图 16-67　协议选择

03 在“添加网络实体”对话框中，选择“新建→计算机”命令（如图 16-68 所示）。在“新建计算机规则元素”对话框中，设置名称为“服务器 1”、IP 地址为 192.168.100.10，如图 16-69 所示。

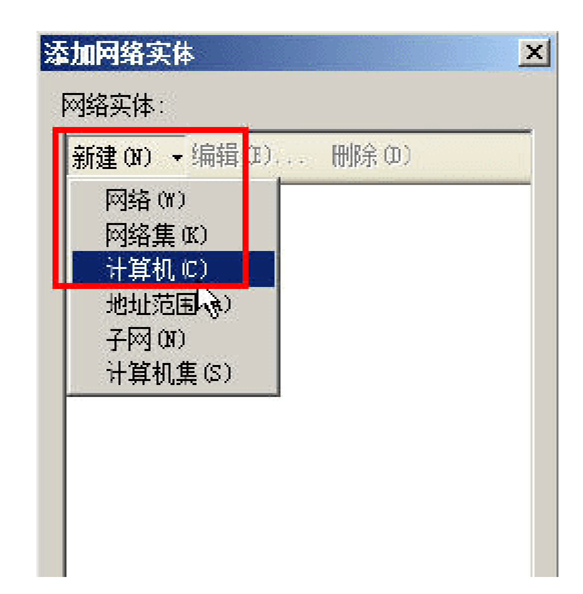


图 16-68　新建计算机

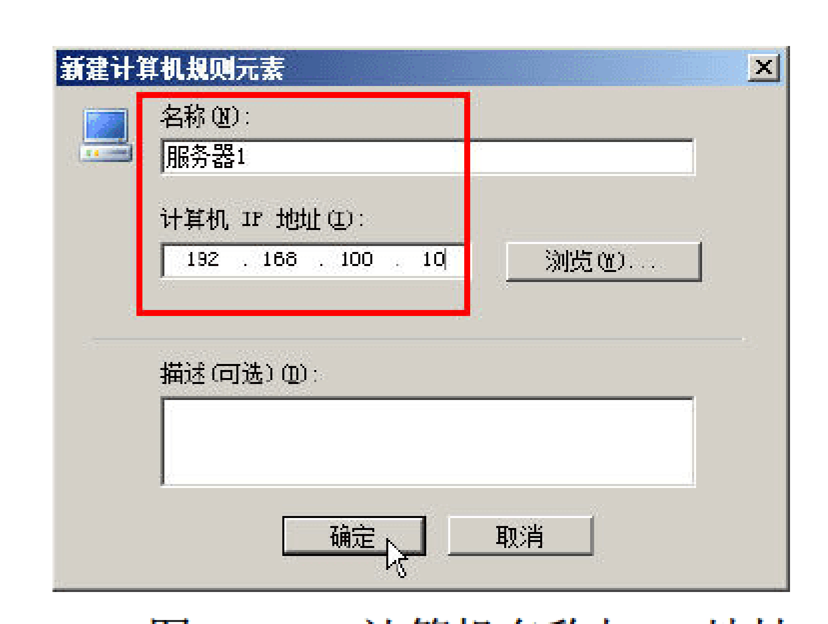


图 16-69　计算机名称与 IP 地址

04 然后在“访问规则源”对话框中，添加“服务器 1”，如图 16-70 所示。

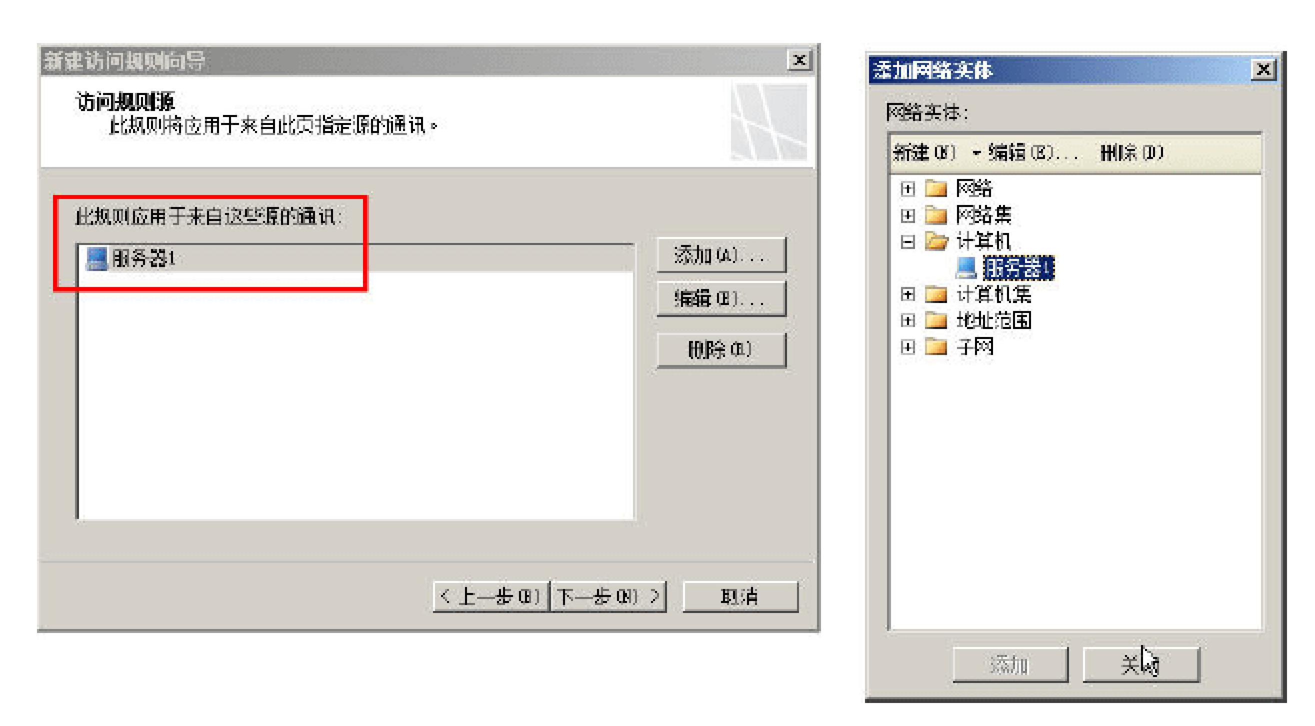


图 16-70 访问规则源

4. 电子邮件服务器发布规则的创建

接下来创建服务器发布规则 1：发布电子邮件服务器到 192.168.100.10。

01 在 Forefront TMG 控制台中，右击“防火墙策略”，在弹出的快捷菜单中选择“新建→邮件服务器发布规则”命令，如图 16-71 所示。

02 在“欢迎使用新建邮件服务器发布规则向导”对话框中，设置发布规则的名称为“发布邮件服务器到 192.168.100.10”，如图 16-72 所示。



图 16-71 新建邮件服务器发布规则

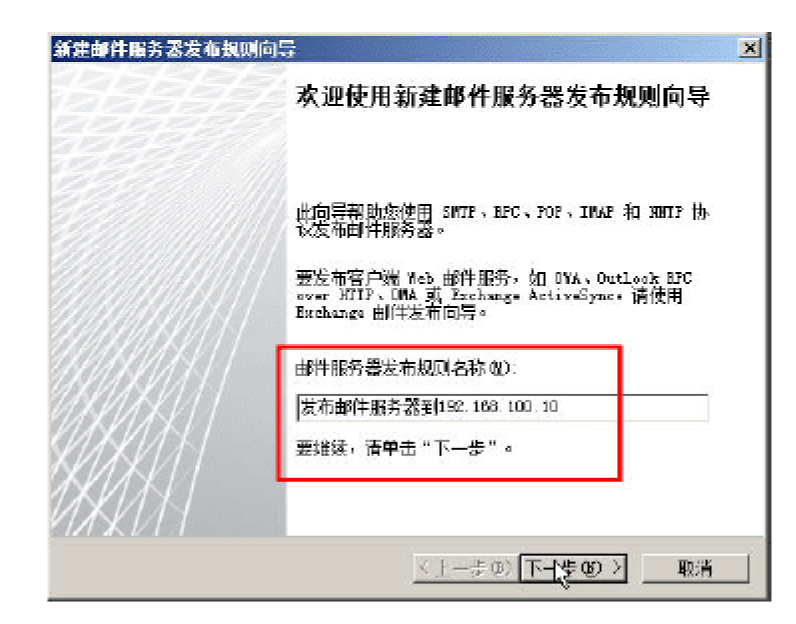


图 16-72 设置发布规则名称

03 在“选择访问类型”对话框中，选中“客户端访问：RPC、IMAP、POP3、SMTP”单选按钮，如图 16-73 所示。

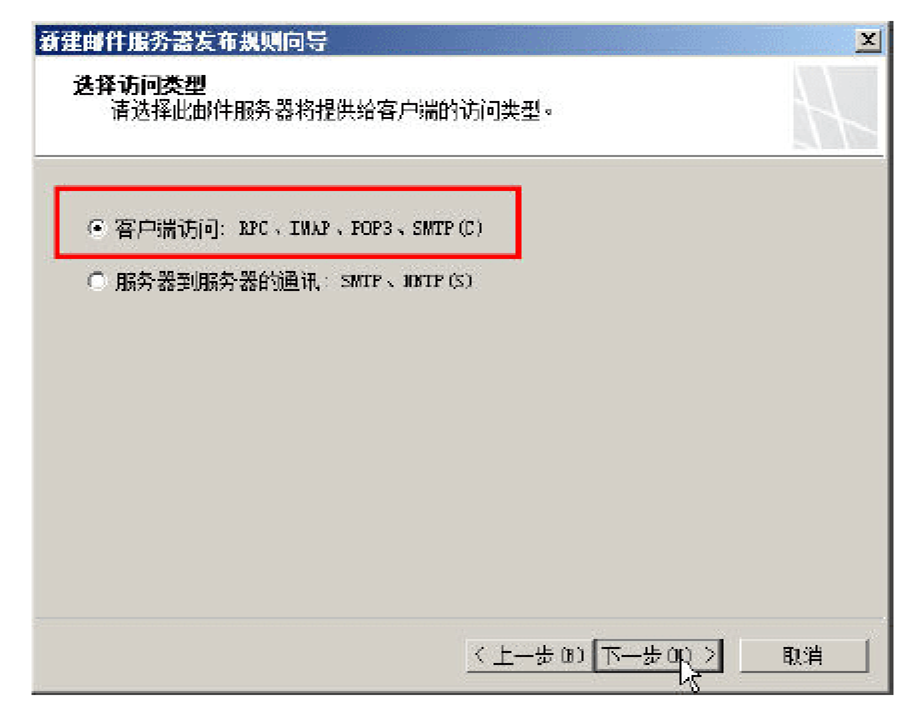


图 16-73

04 在“客户端访问”对话框中，选中“POP3”与“SMTP”复选框，如图 16-74 所示。如

果邮件服务器还有其他协议，例如安全 POP3、安全 SMTP，或 IMAP4 等，可根据需要选择。

05 在“选择服务器”对话框中，指定要发布的服务器的地址，本例为 192.168.100.10，如图 16-75 所示。

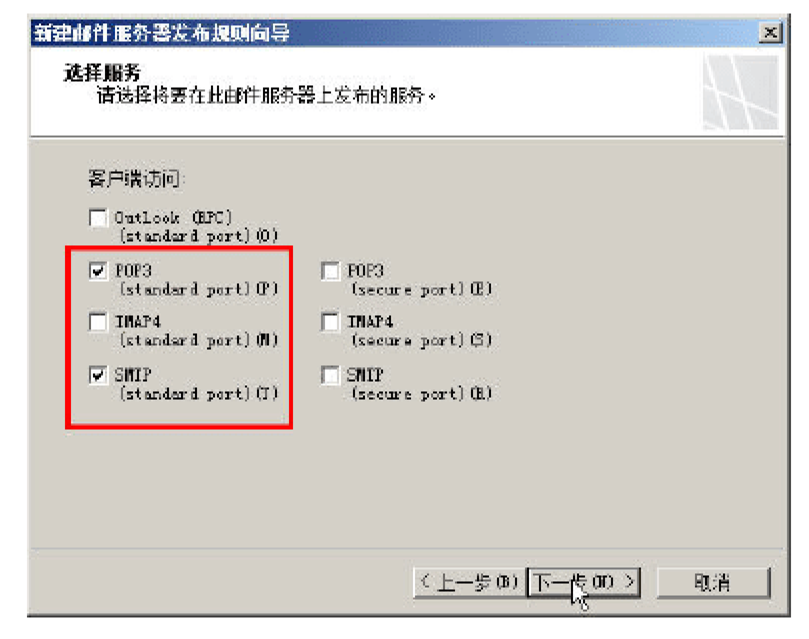


图 16-74　选择协议

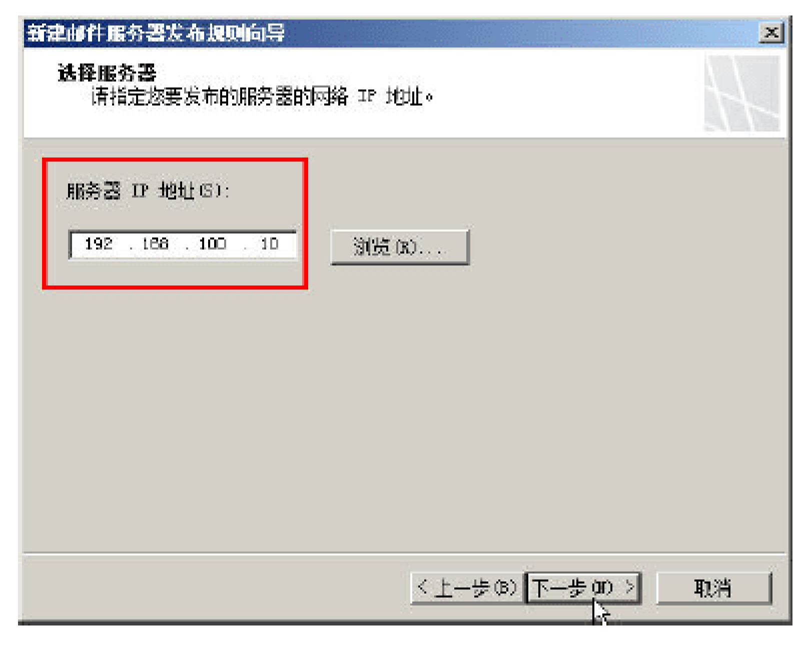


图 16-75　指定要发布的服务器的地址

06 在“网络侦听器 IP 地址”对话框中，选中“外部”复选框，如图 16-76 所示。

07 在“正在完成新建 邮件服务器发布规则向导”对话框中，单击“完成”按钮，如图 16-77 所示。

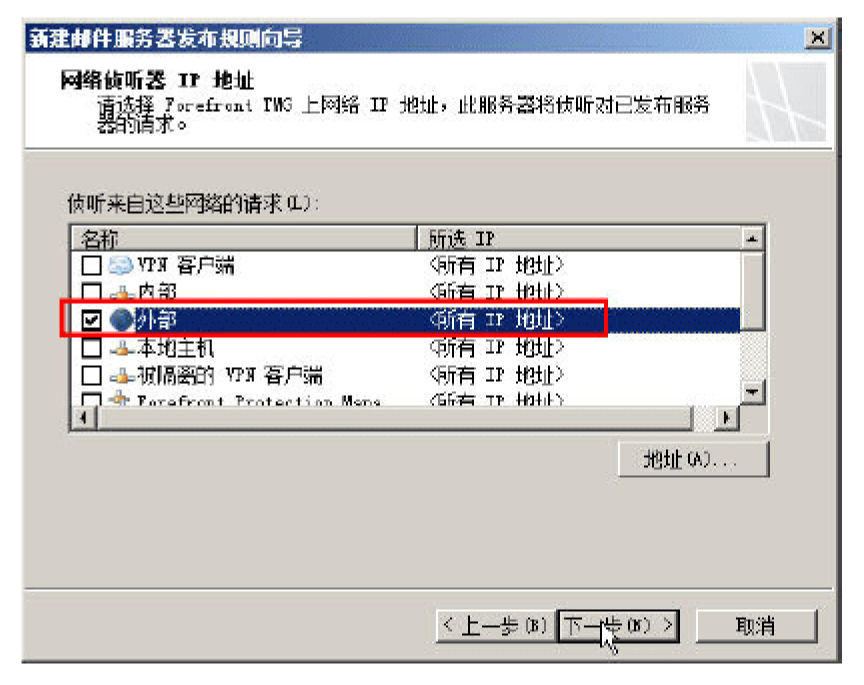


图 16-76　选择网络侦听器

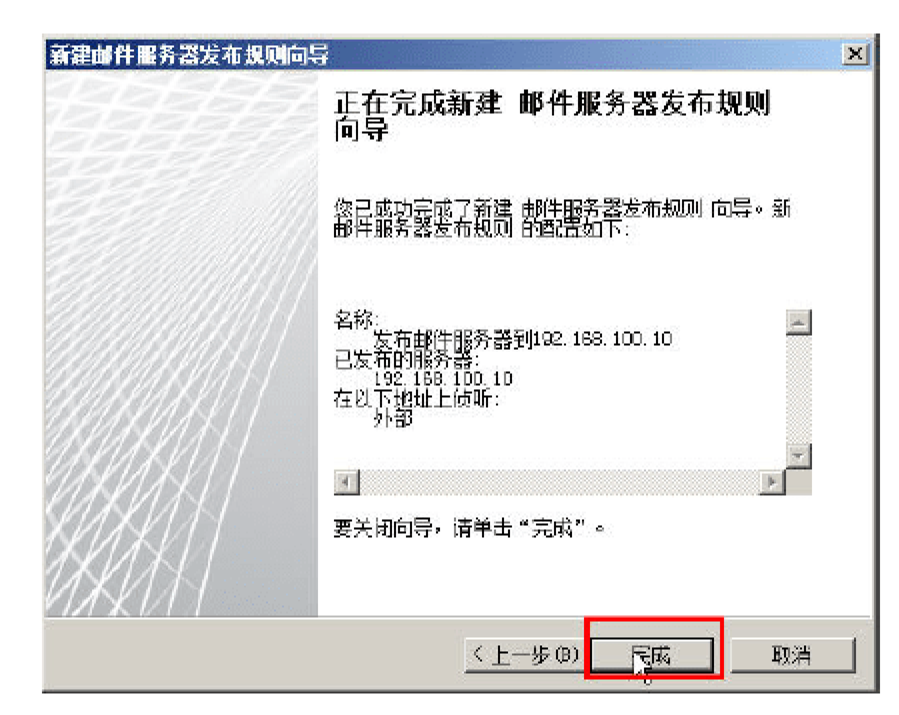


图 16-77　完成邮件服务器发布规则

5. 发布 Web 服务器到 192.168.100.10

创建服务器发布规则 2：发布 Web 服务器到 192.168.100.10，域名为 mail.msft.com（假设该邮件服务器对外提供的域名是 mail.msft.com）。

在创建 Web 服务器发布规则时，需要使用“Web 侦听器”，如果没有 Web 侦听器，可以在创建规则的过程中创建，也可以提前创建。创建的 Web 侦听器，可以发布多个 Web 服务器。

01 在 Forefront TMG 控制台中，右击“防火墙策略”，在弹出的快捷菜单中选择“新建→网站发布规则”命令，如图 16-78 所示。

02 在“欢迎使用新建 Web 发布规则向导”对话框中，在“Web 发布规则名称”文本框中，输入这次创建的规则的名称，在本例中为“发布 mail.msft.com 到 192.168.100.10”，如图 16-79 所示。




图 16-78 创建网站发布规则

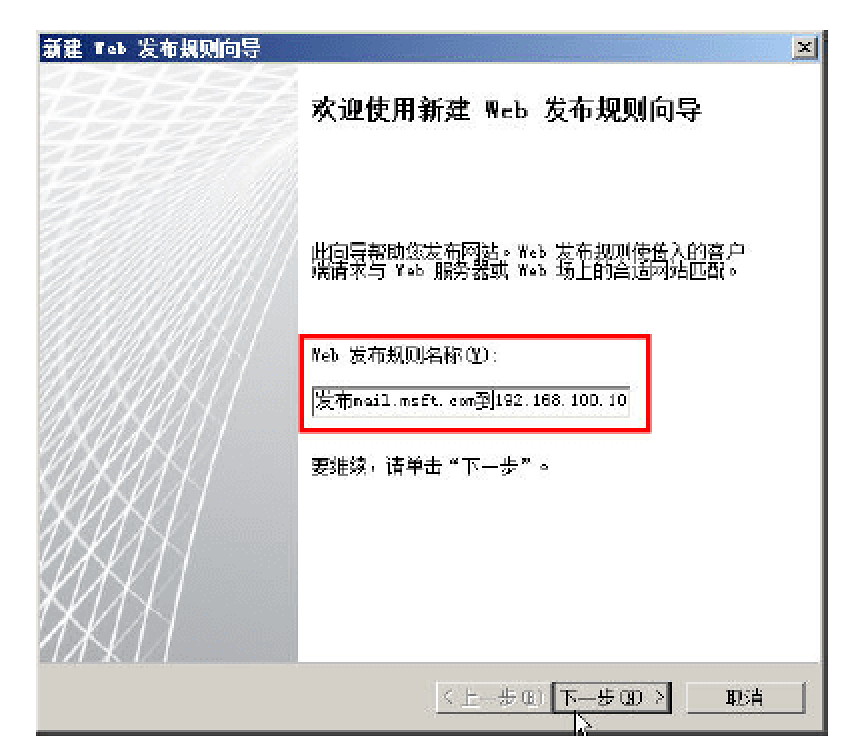


图 16-79　设置发布规则名称

03 在“请选择规则操作”对话框中，选中“允许”单选按钮，如图 16-80 所示。

04 在“发布类型”对话框中，选中“发布单个网站或负载平衡器”单选按钮，如图 16-81 所示。

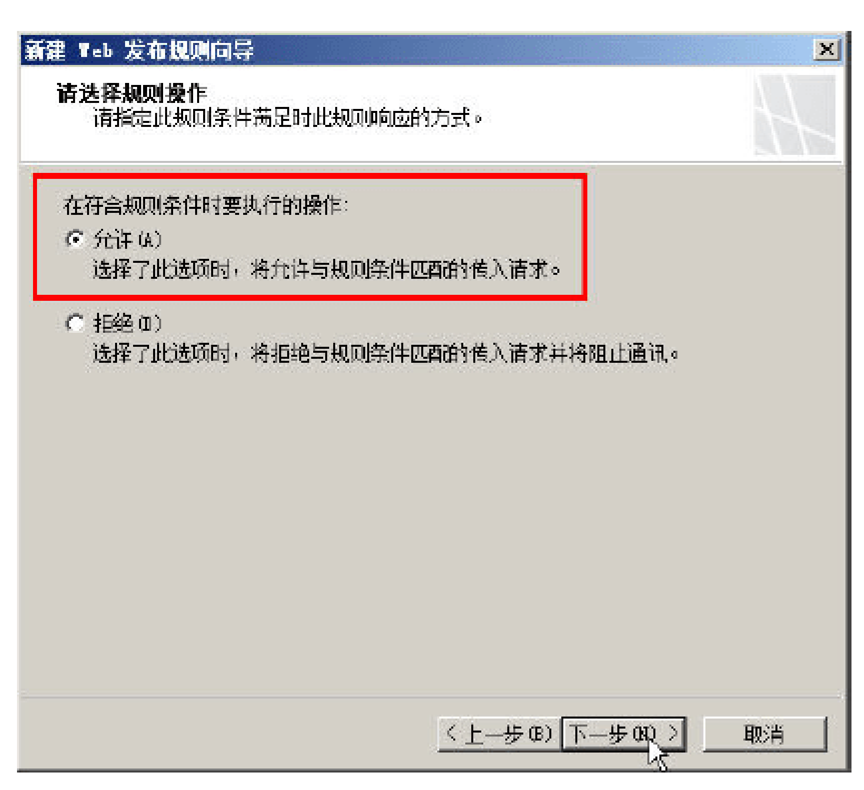


图 16-80 允许

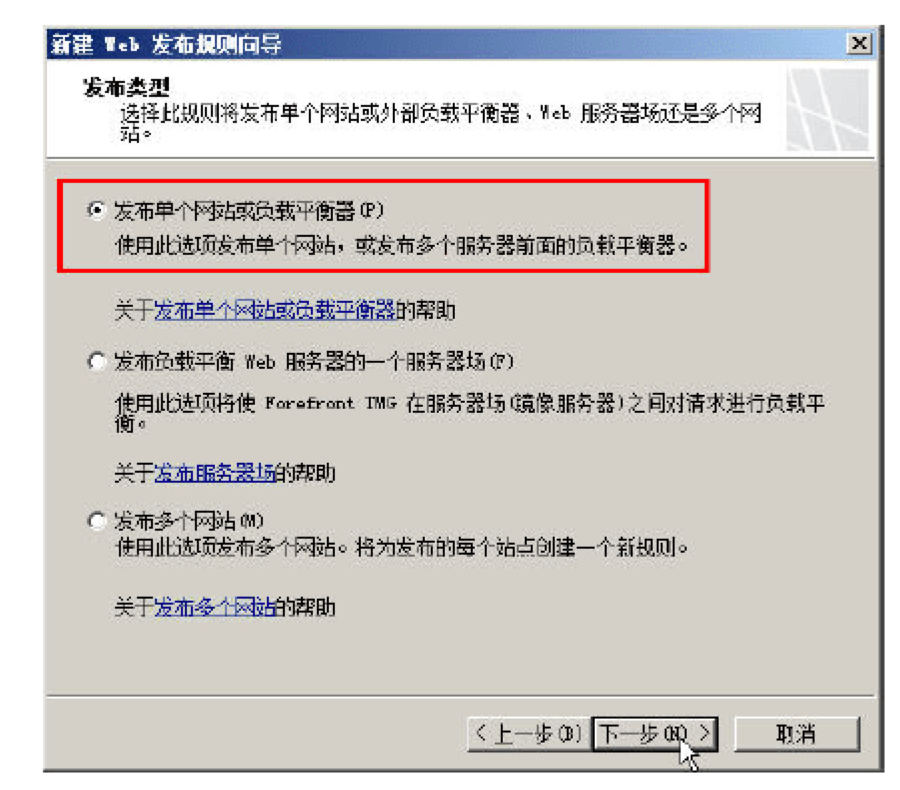


图 16-81　发布类型

05 在“服务器连接安全”对话框中，选中“使用不安全的连接连接发布的 Web 服务器或服务器场”单选按钮，如图 16-82 所示。

06 在“内部发布详细信息”对话框中，设置“内部站点名称”，并且选中“使用计算机名称或 IP 地址连接到发布的服务器”复选框，并在“计算机名称或 IP 地址”文本框中，输入当前要发布的服务器的地址，本例为 192.168.100.10，如图 16-83 所示。

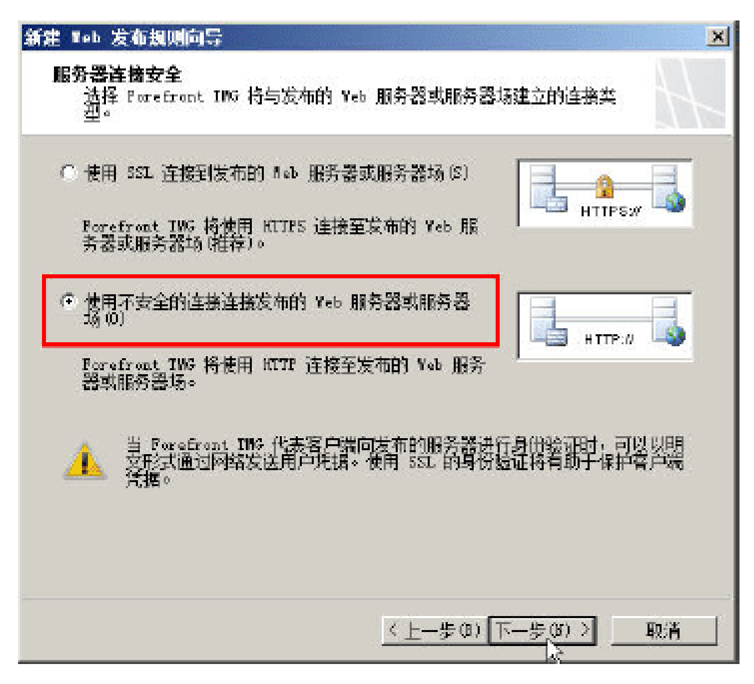


图 16-82　服务器连接安全

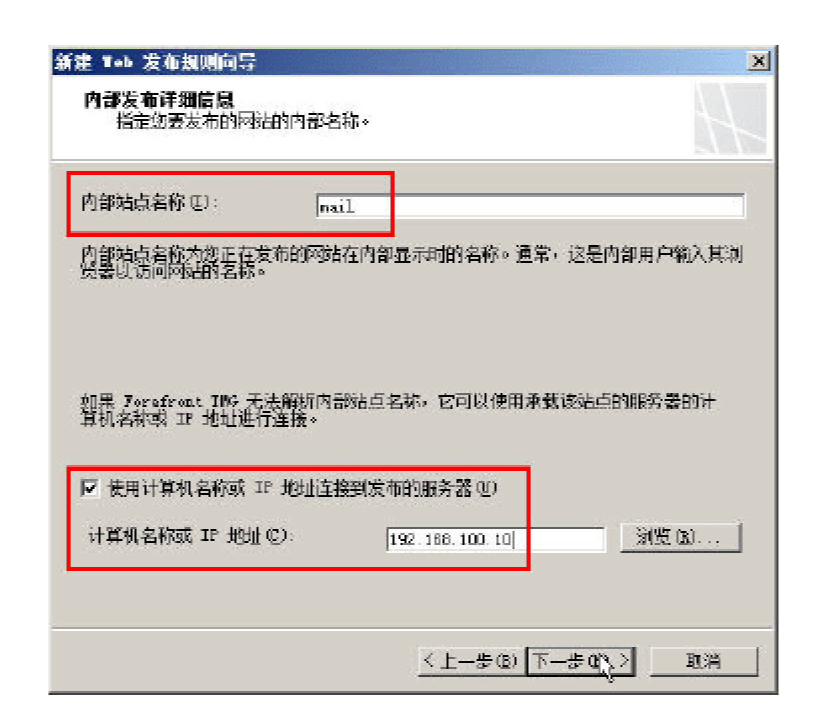
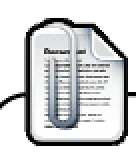


图 16-83　指定要发布的服务器的 IP 地址

07 在“内部发布详细信息”对话框中，在“路径（可选）”文本框中输入“/*”，如图 16-84 所示。



说 明

如果要将同一台计算机的多个 Web 服务器发布到 Internet，则需要选中“转发原始主机头而不是前一页的内部站点名称字段中指定的实际主机头”复选框，并且在发布的 Web 服务器中，使用“主机头名”的方式创建网站。

08 在“公共名称细节”对话框中，在“接受请求”下拉列表中选择“此域名（在以下输入）”选项，然后在“公用名称”文本框中输入本次发布的域名 “mail.msft.com”，如图 16-85 所示。

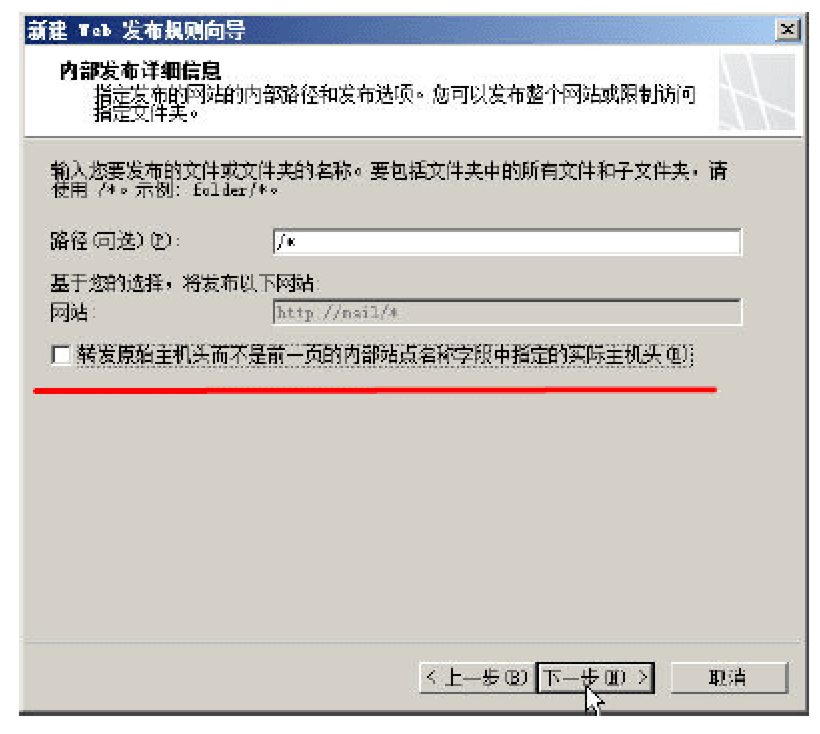


图 16-84 发布路径

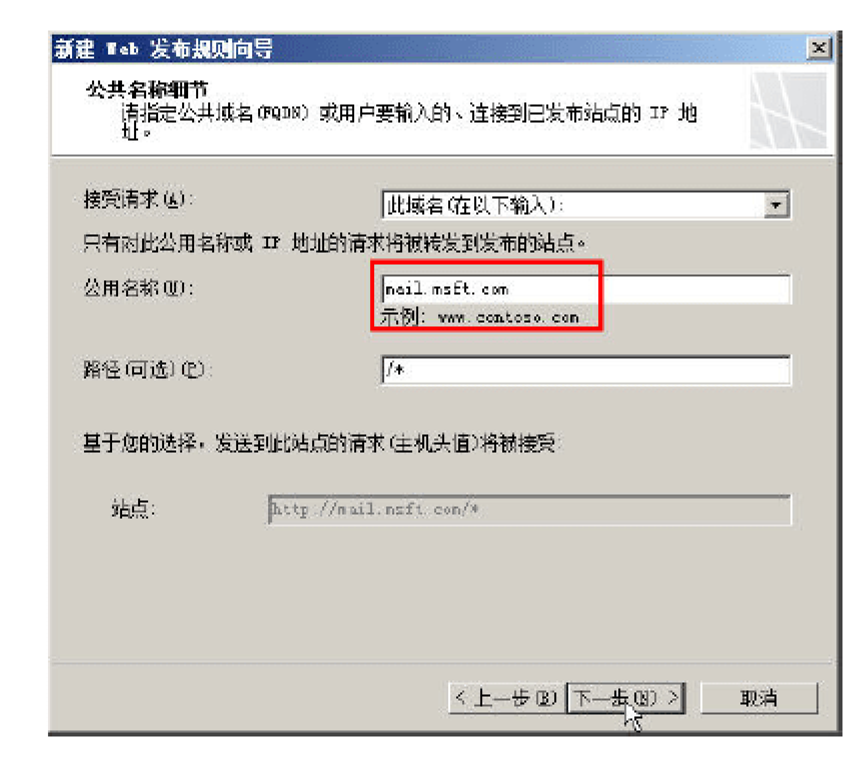


图 16-85 指定要发布的域名



说 明

如果的网络中只有一台 Web 服务器，并且这台服务器上具有多个网站，可以在“接受请求”下拉列表中选择“所有请求”选项。

09 在“选择 Web 侦听器”对话框中，选择要使用的 Web 侦听器。因为这是一台新安装的 Forefront TMG，还没有侦听器，所以需要先创建一个。单击“新建”按钮，进入“新建 Web 侦听器向导”对话框，在“Web 侦听器名称”文本框中，输入新建的 Web 侦听器的名称，本例为“Web Detect”，如图 16-86 所示。

10 在“客户端连接安全设置”对话框中，选中“不需要与客户端建立 SSL 安全连接”单选按钮，如图 16-87 所示。

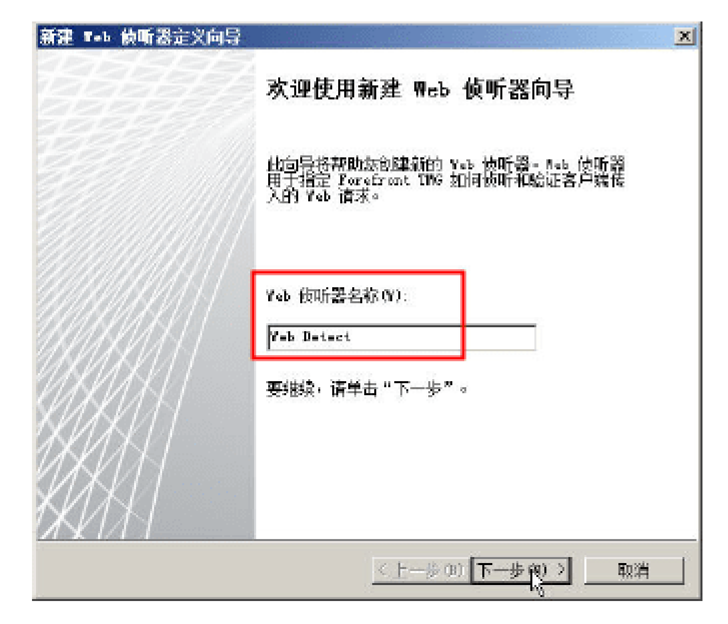


图 16-86 指定 Web 侦听器名称

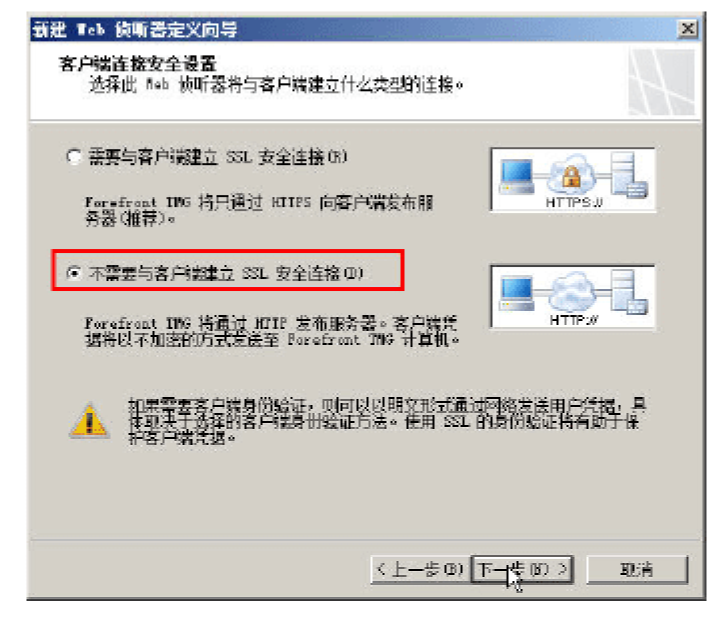


图 16-87 客户端连接安全设置

11 在“Web 侦听器 IP 地址”对话框中，选中“外部”复选框，如图 16-88 所示。

12 在“身份验证设置”对话框中，选择“没有身份验证”选项，如图 16-89 所示。

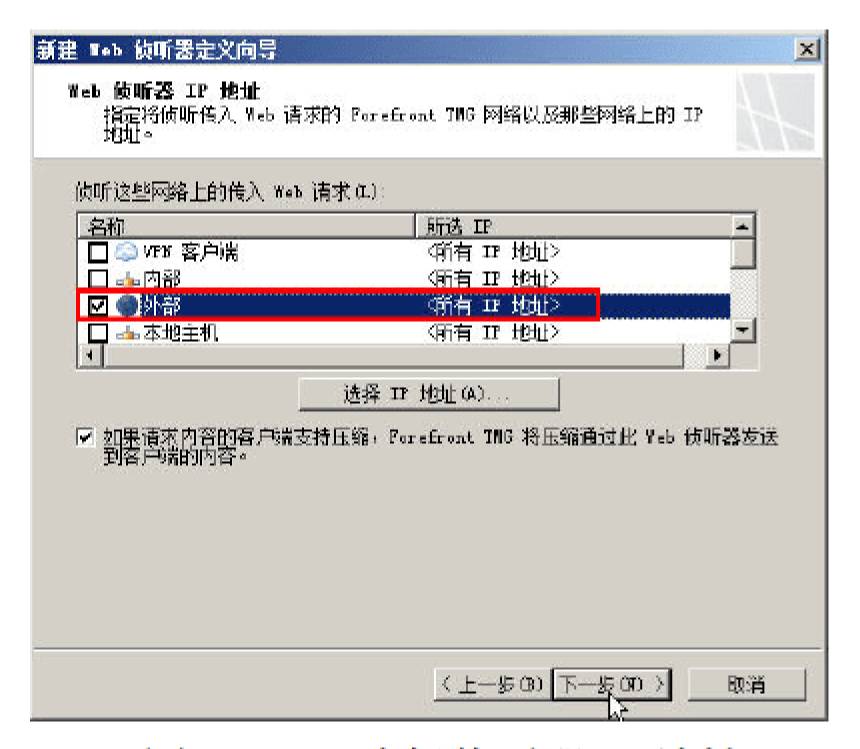


图 16-88 选择侦听器 IP 地址



图 16-89 身份验证方式

13 在“单一登录设置”对话框中，选择默认值，如图 16-90 所示。

14 在“正在完成新建 Web 侦听器向导”对话框中，单击“完成”按钮，如图 16-91 所示。

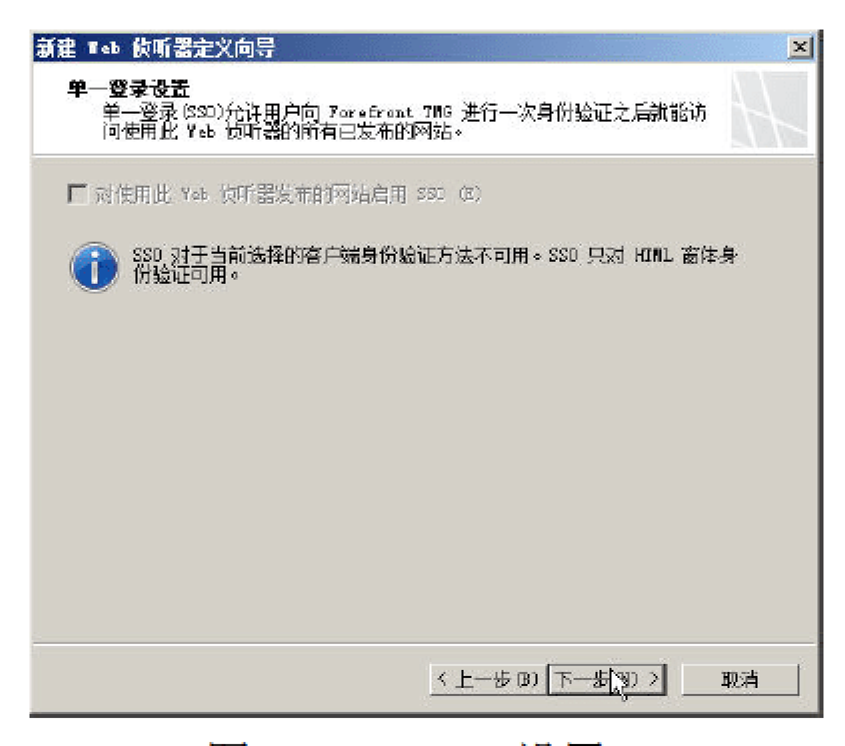


图 16-90 SSO 设置

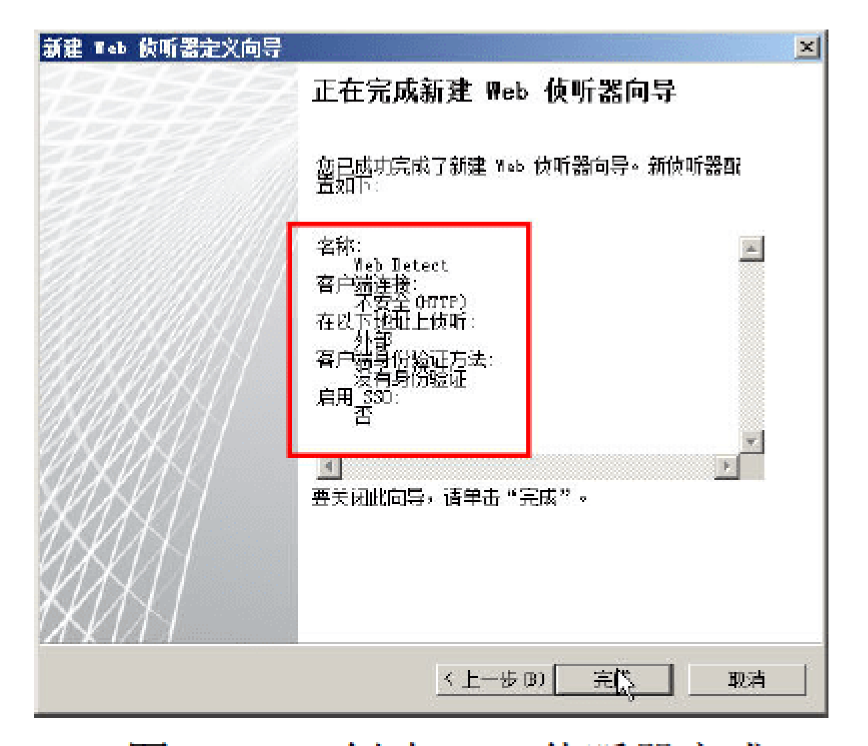


图 16-91 创建 Web 侦听器完成

15 创建完 Web 侦听器后，返回到“选择 Web 侦听器”对话框中，选择新创建的 Web 侦听器，如图 16-92 所示。

16 在“身份验证委派”对话框中，选择“无委派，但是客户端可以直接进行身份验证”选项，如图 16-93 所示。

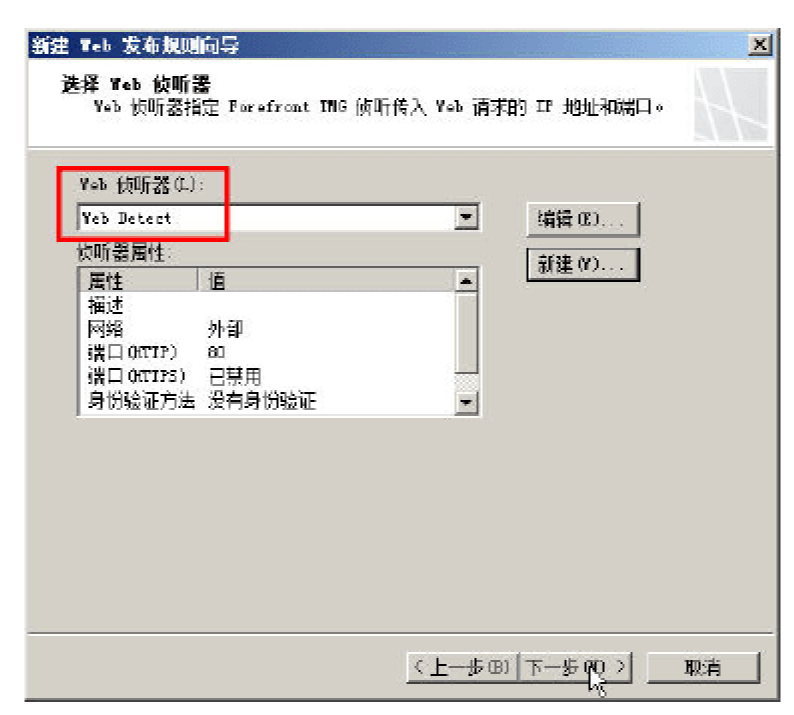


图 16-92 选择 Web 侦听器

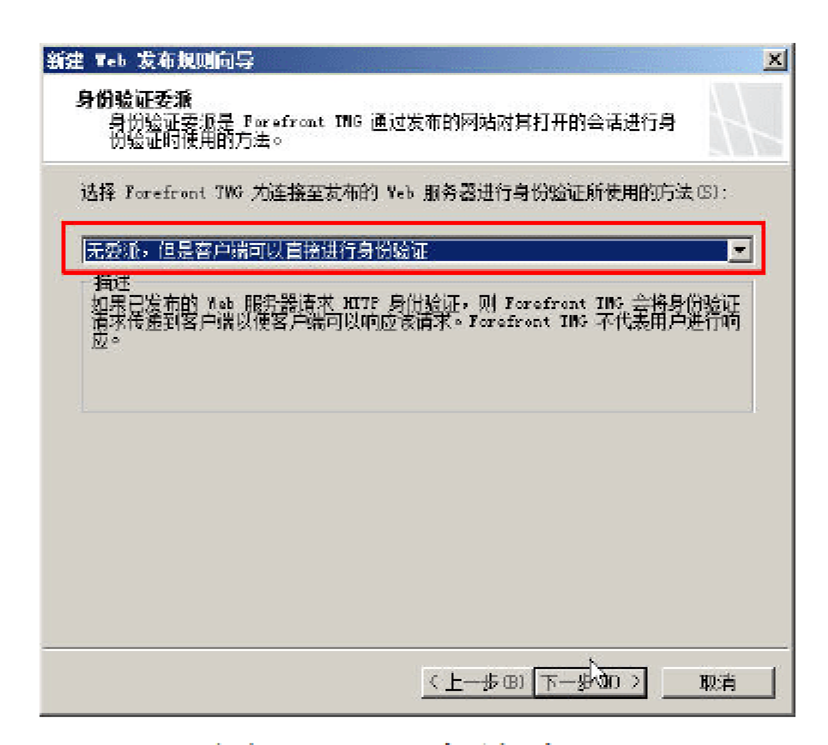


图 16-93 身份验证



说　明

如果发布的是普通的、不需要身份验证的网站，则选择“无委派，客户端无法直接进行身份验证”。

17 在“用户集”对话框中，选择默认值，如图 16-94 所示。

18 在“正在完成新建 Web 发布规则向导”对话框中，单击“完成”按钮，规则创建完成，如图 16-95 所示。

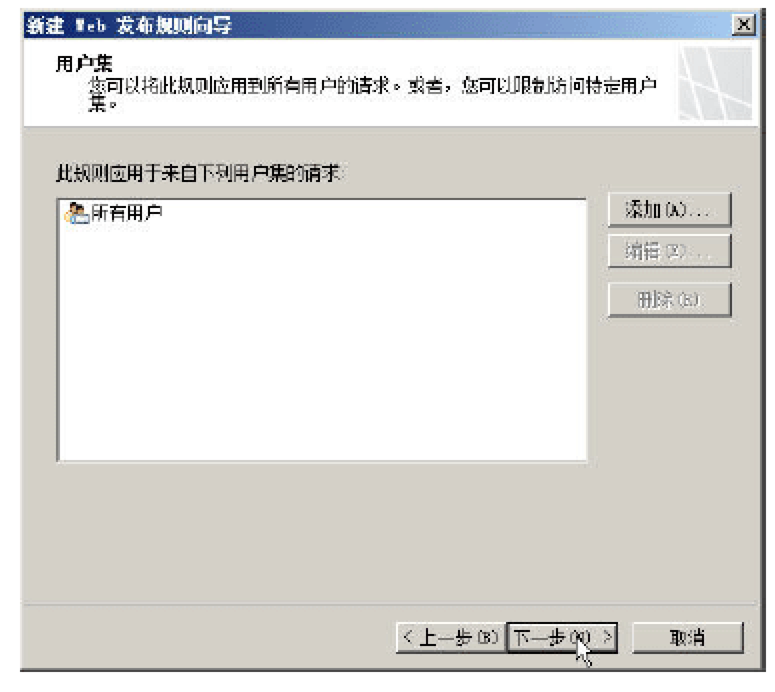


图 16-94　用户集

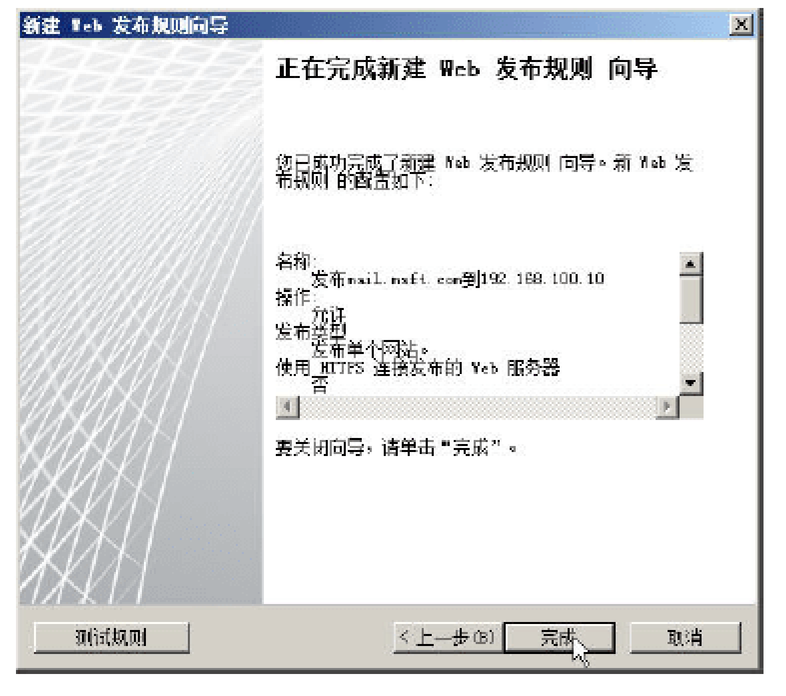


图 16-95　完成 Web 服务器发布规则

6. 创建访问规则 4

创建访问规则 4（允许服务器 2：192.168.100.11 以 HTTP 协议访问“外部”）与访问规则 3 的创建类似，只是以下几点不同。

01 在“欢迎使用新建访问规则向导”对话框中，访问规则名称为“允许服务器 2 以 HTTP 协议访问外部”，如图 16-96 所示。当然，也可以设置一个其他的名称，只要能让用户明白你所创建规则的意义即可。

02 单击“下一步”按钮，在“协议”对话框中选择 HTTP，如图 16-97 所示。

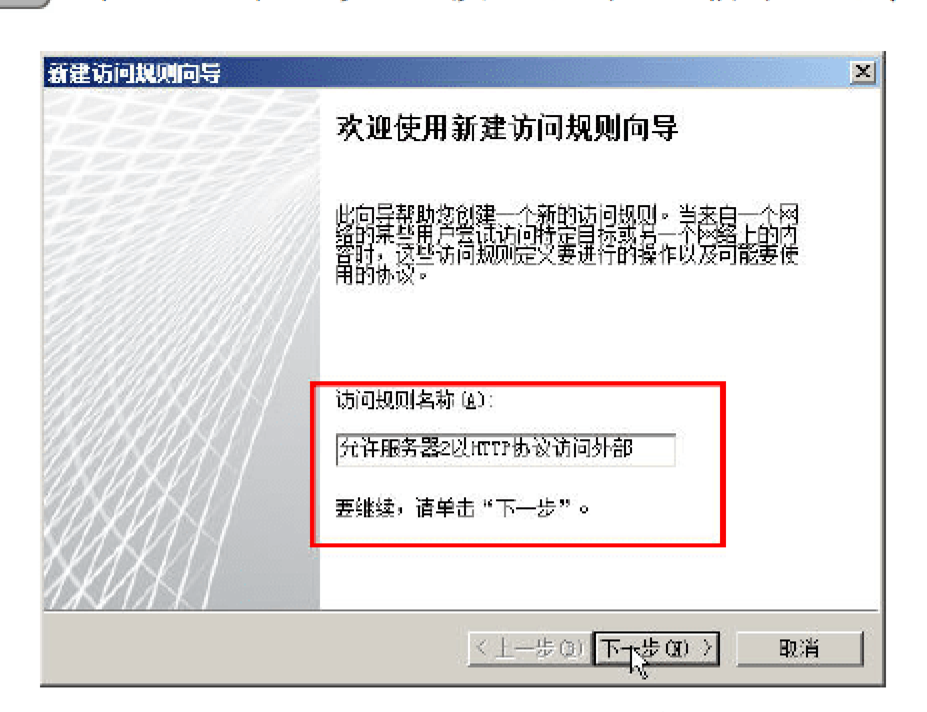


图 16-96　创建规则名称

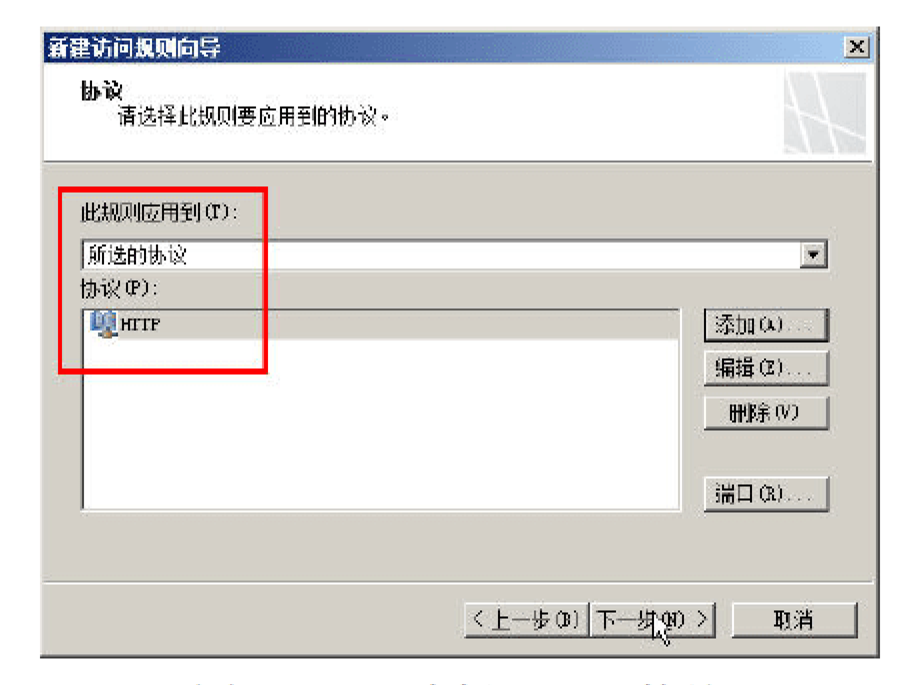


图 16-97　选择 HTTP 协议

03 在“访问规则源”对话框中，将“源”改为“服务器 2”，如图 16-98 所示。用户需要在“添加网络实体”中添加计算机对象，名称为“服务器 2”，IP 地址为 192.168.100.11。

04 其他的操作与访问规则 3 相同，不再赘述。

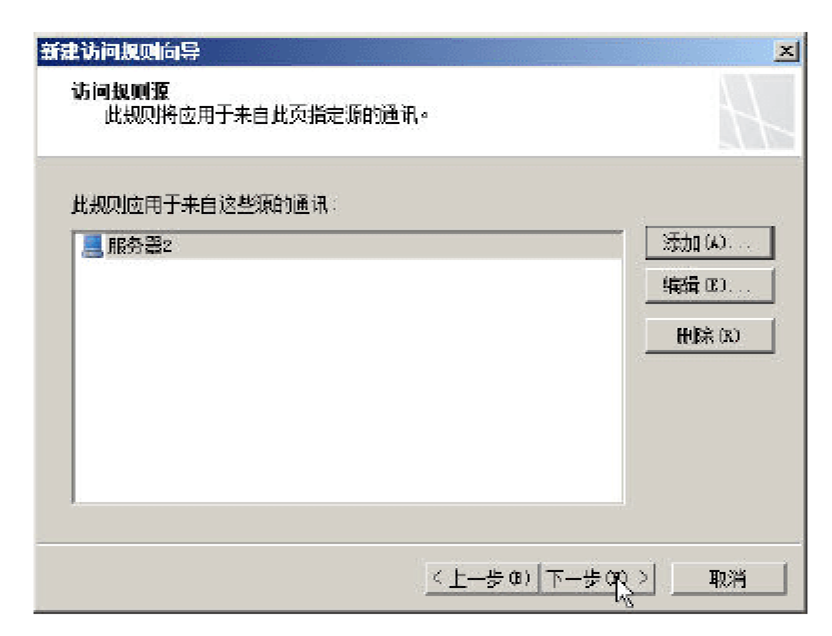


图 16-98 指定源

7. 创建访问规则 5

创建访问规则 5（拒绝服务器 3：192.168.100.20 以“任何协议”访问“外部”）与以前创建的访问规则类似，只是以下几点不同。

01 在“欢迎使用新建访问规则向导”对话框中，访问规则名称为“拒绝服务器 3 访问外部”，如图 16-99 所示。

02 在“规则操作”对话框中，选中“拒绝”单选按钮，如图 16-100 所示。

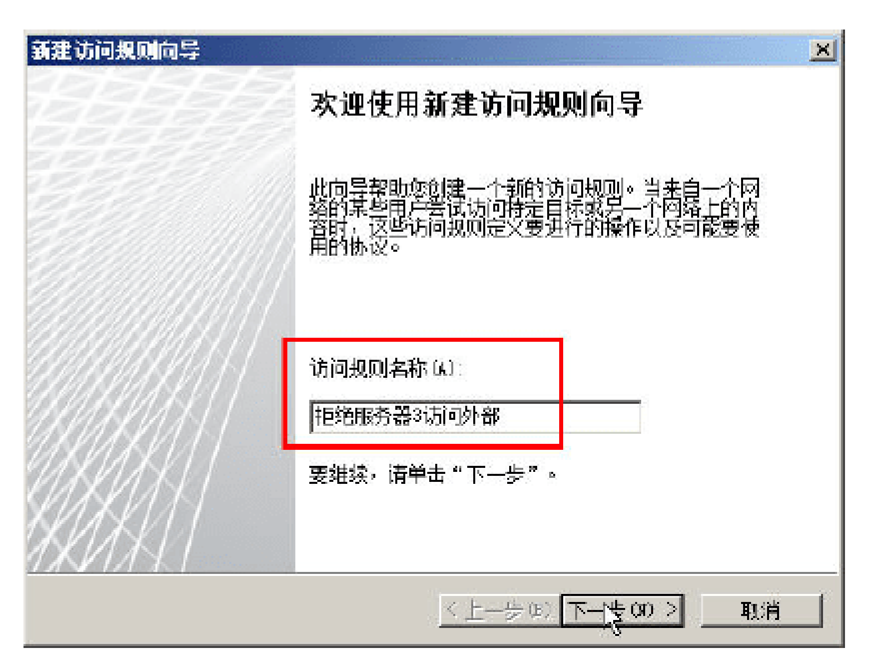


图 16-99 规则名称

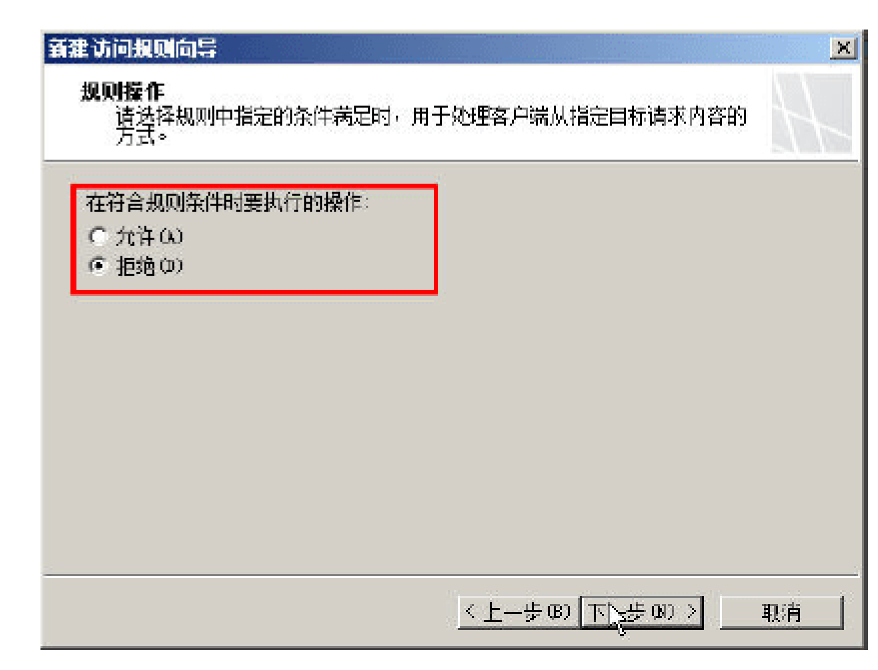


图 16-100 拒绝

03 在“协议”对话框中选中“所有出站通讯”选项，如图 16-101 所示。

04 在“访问规则源”对话框中，单击“添加”按钮，在弹出的“新建计算机规则元素”对话框中，添加名为“服务器 3”、IP 地址为 192.168.100.20 的计算机对象，如图 16-102 所示。并添加到“源”列表中。

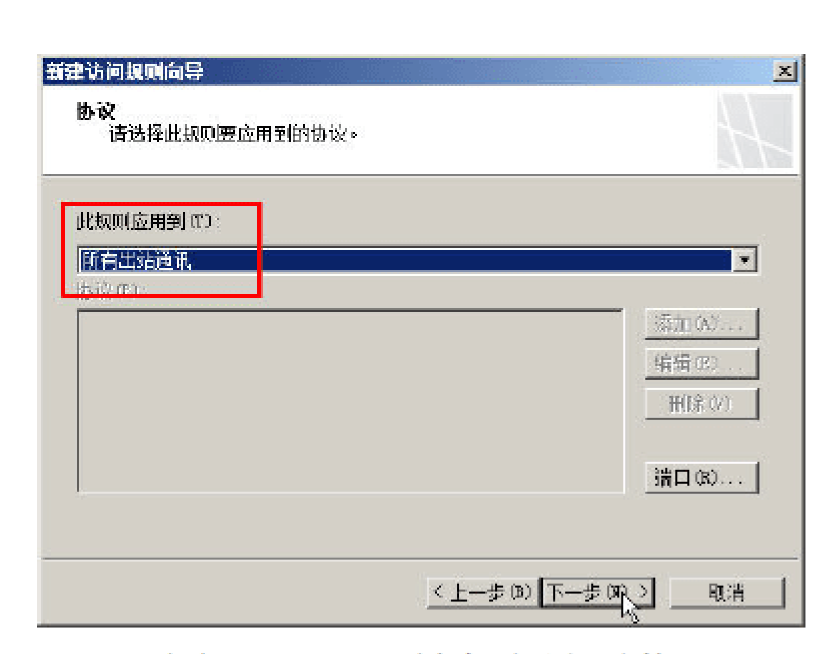


图 16-101 所有出站通信

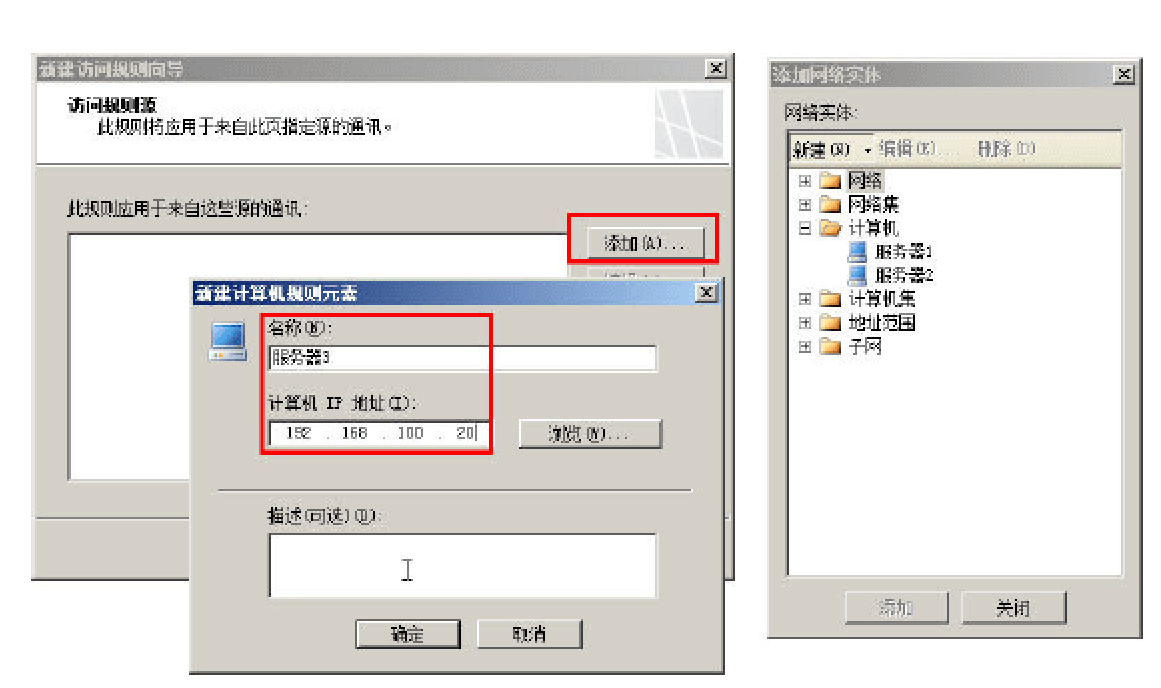


图 16-102 添加服务器 3 对象

8. 发布 Web 服务器到 192.168.100.20

创建服务器发布规则 3（发布 Web 服务器到 192.168.100.20，域名为 www.msft.com）与发布规则 2 类似，只是以下几点不同。

01 在 Forefront TMG 中，创建 Web 服务器发布规则，设置规则名称为“发布 Web 服务器到 192.168.100.20”，如图 16-103 所示。

02 在“内部发布详细信息”对话框中，选中“使用计算机名称或 IP 地址连接到发布的服务器”复选框，并且设置计算机名称为 192.168.100.20，如图 16-104 所示。

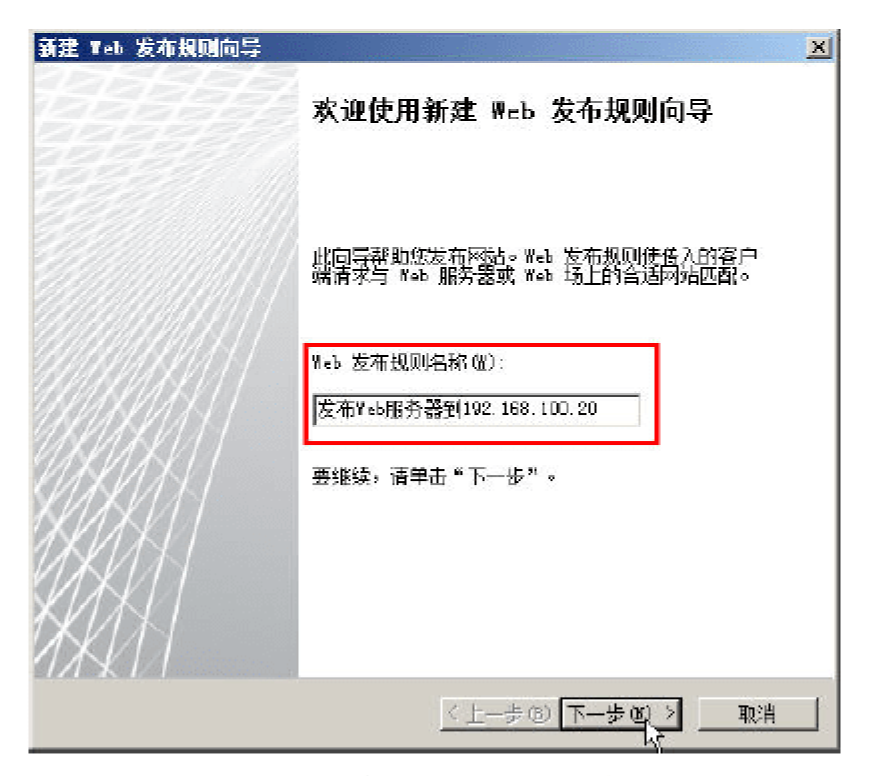


图 16-103　发布规则名称

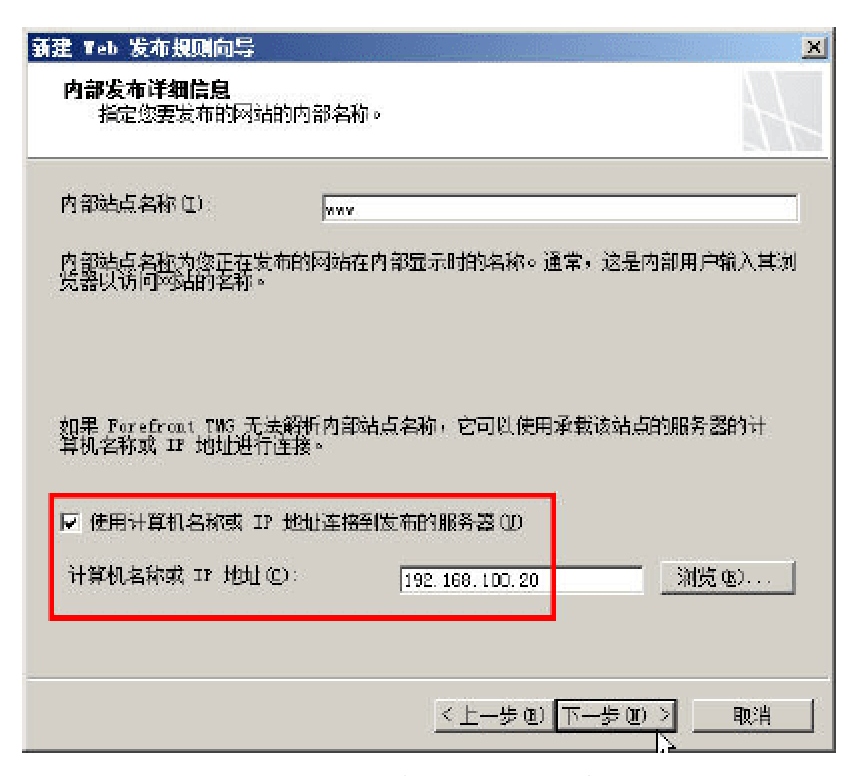


图 16-104　指定要发布的服务器的 IP 地址

03 在“公共名称细节”对话框中，设置公用名称为 www.msft.com，如图 16-105 所示。

04 在“身份验证委派”对话框中，选择“无委派，客户端无法直接进行身份验证”选项，如图 16-106 所示。

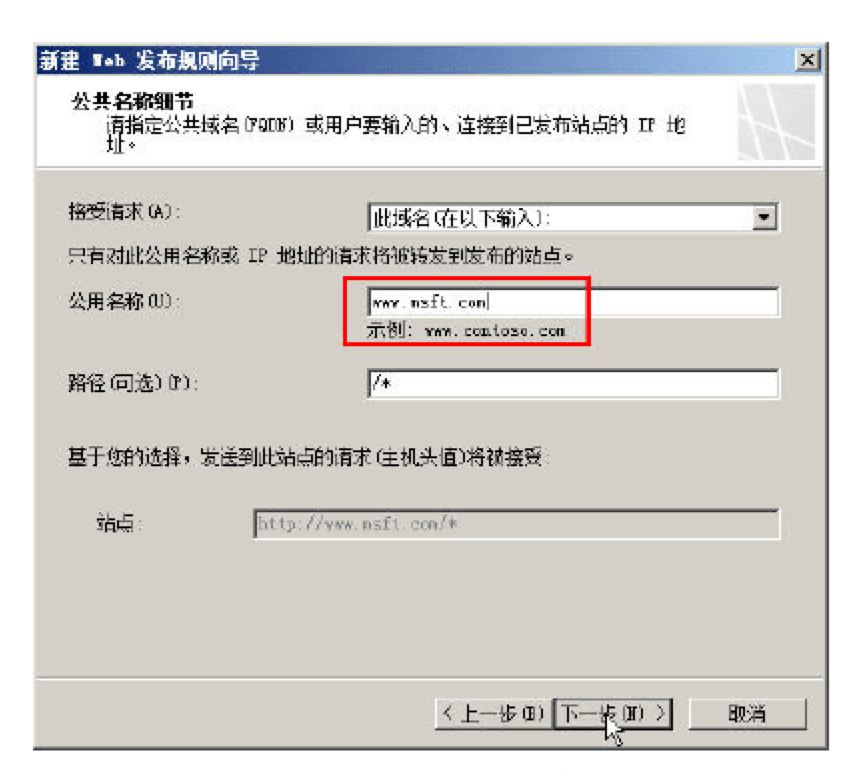


图 16-105　公共名称细节

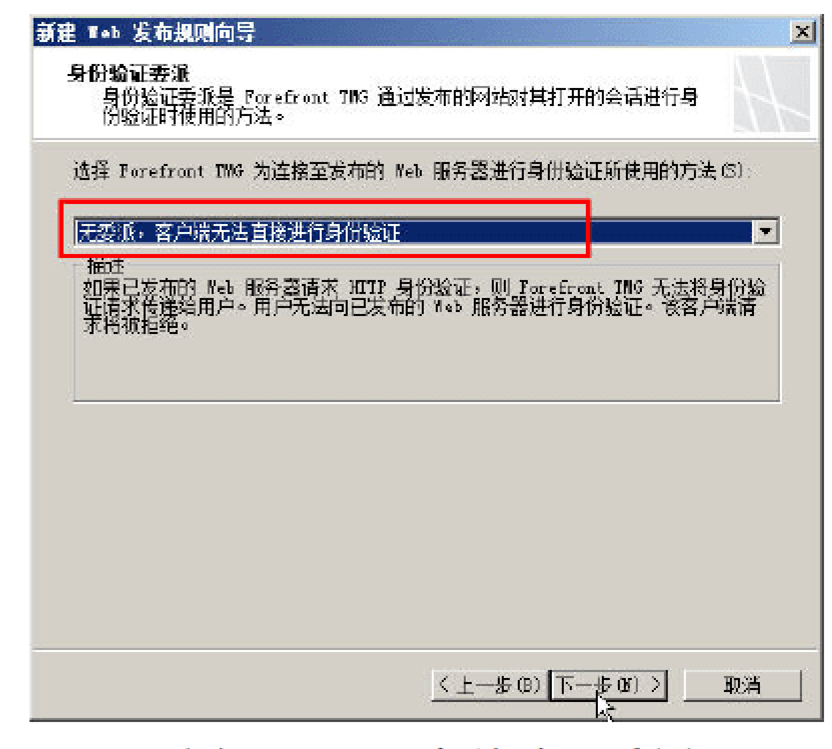


图 16-106　身份验证委派

9. 发布 FTP 服务器

发布 FTP 服务器到 192.168.100.20 的步骤如下。

01 在 Forefront TMG 控制台中，在“防火墙策略”中，选择“新建→非 Web 服务器协议发布规则”命令，如图 16-107 所示。

02 在“欢迎使用新建服务器发布规则向导”对话框中，在“服务器发布规则”文本框中，

输入规则名称为“发布 FTP 服务器到 192.168.100.20”，如图 16-108 所示。

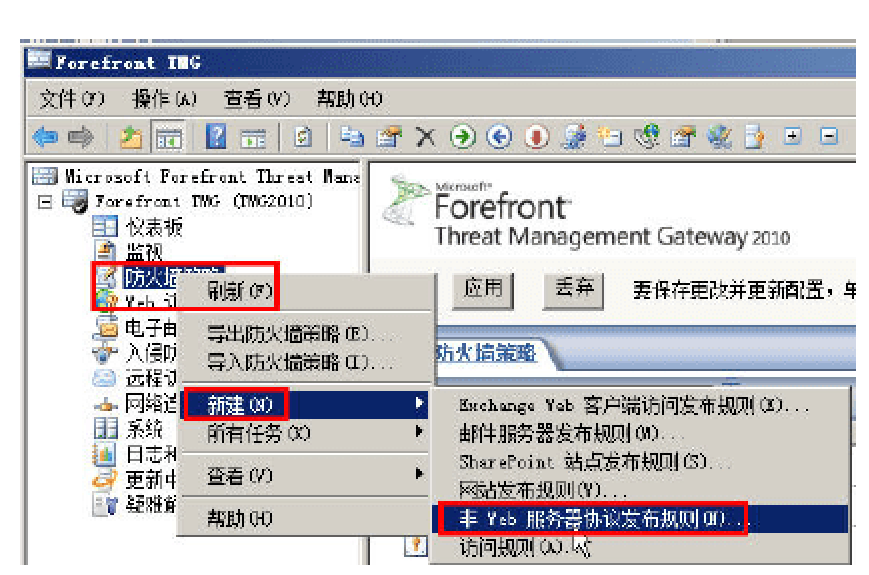




图 16-107　新建非 Web 服务器发布规则

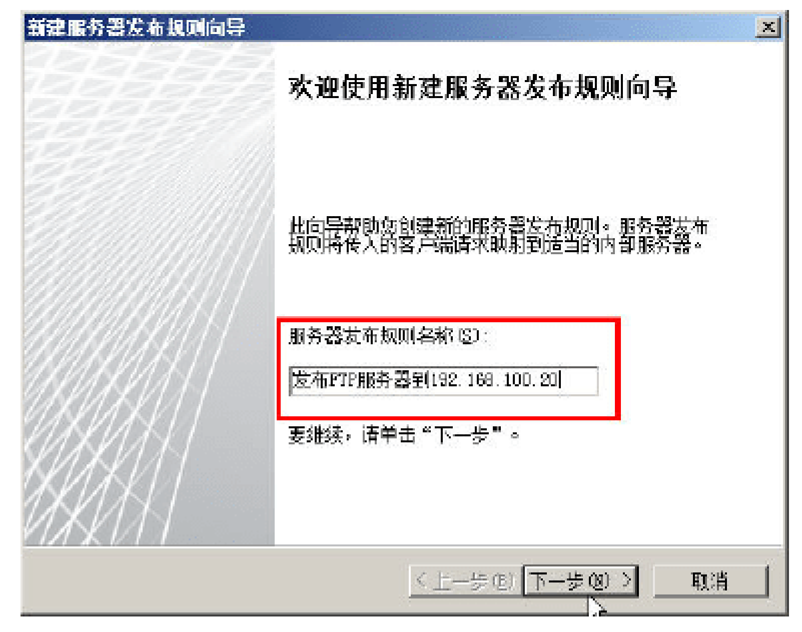


图 16-108　设置规则名称

03 在“选择服务器”对话框中，指定 FTP 服务器的地址为 192.168.100.20，如图 16-109 所示。

04 在“选择协议”对话框中，在“选择的协议”下拉列表中选择“FTP 服务器”选项，如图 16-110 所示。

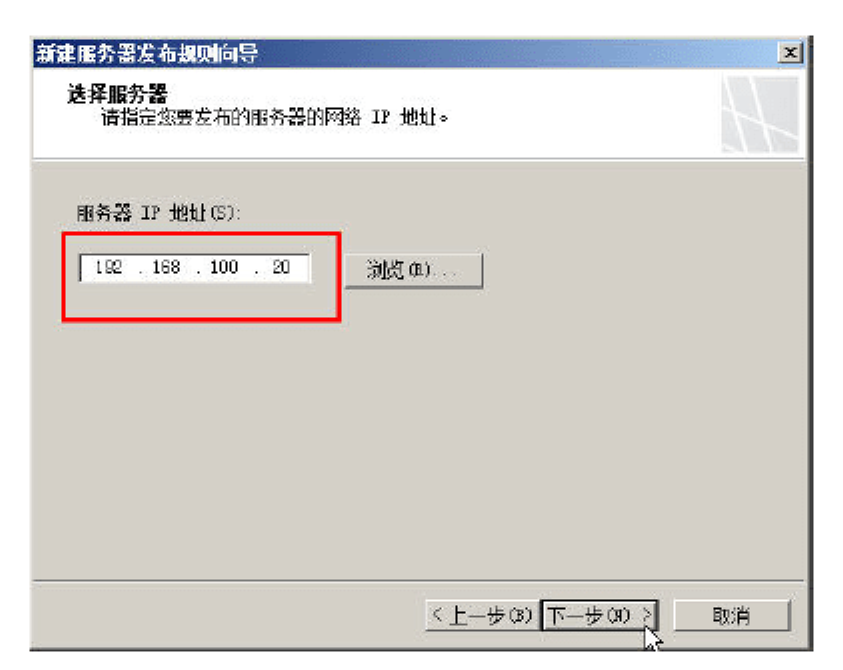


图 16-109　指定要发布的 FTP 服务器地址

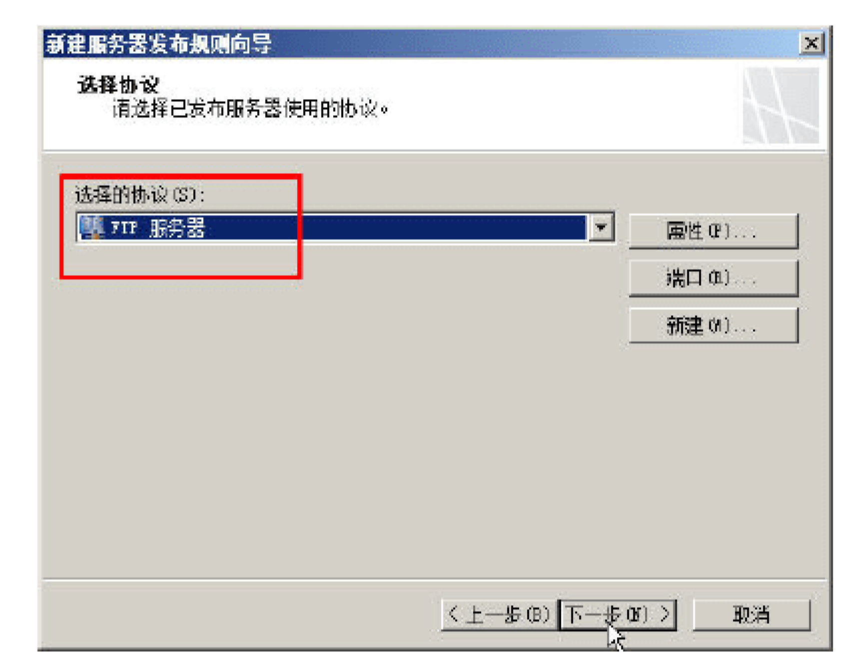


图 16-110　选择 FTP 服务器协议

05 在“网络侦听器 IP 地址”对话框中，选中“外部”复选框，如图 16-111 所示。

06 在“正在完成新建服务器发布规则向导”对话框中，单击“完成”按钮，如图 16-112 所示。

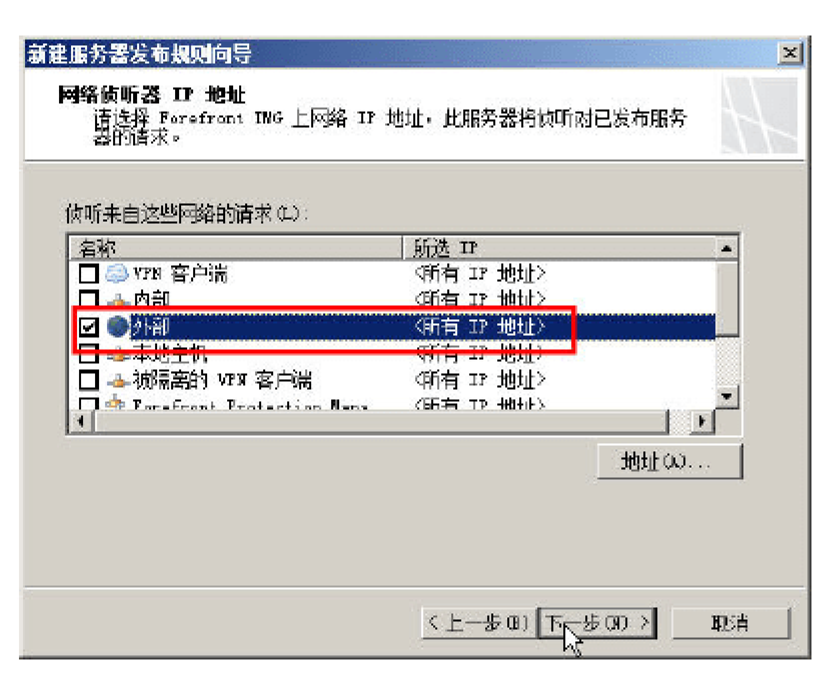


图 16-111　选择侦听器地址

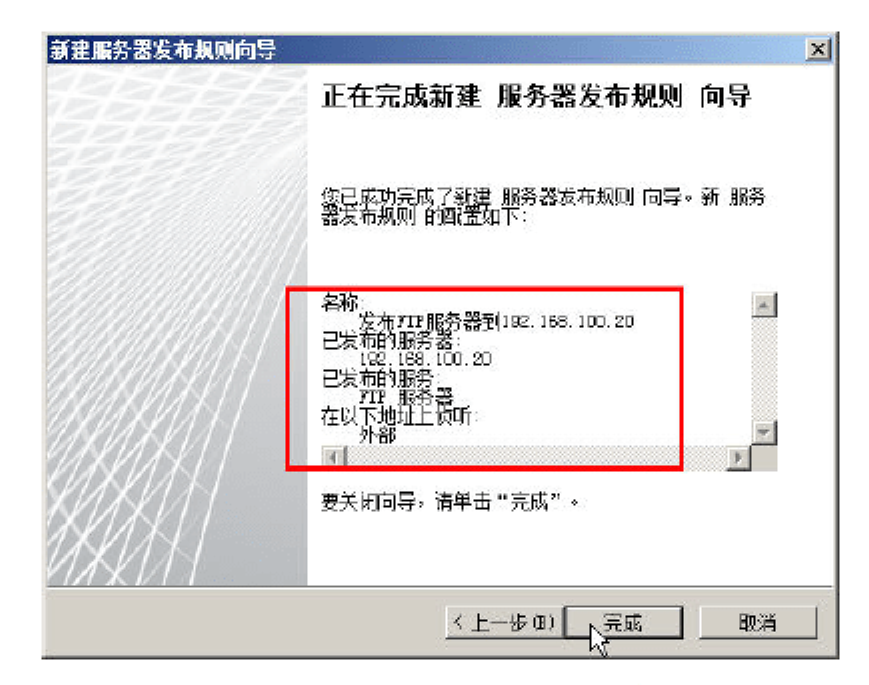


图 16-112　完成规则向导

Forefront TMG 的 FTP 协议使用了“FTP 筛选器”，在默认情况下，FTP 筛选器是以“只读”的方式工作的。如果让用户能上传文件到 FTP 服务器，必须去掉这一设置。

用鼠标右击新创建的 FTP 服务器的发布规则，在弹出的快捷菜单中选择“配置 FTP”命令（如图 16-113 所示），在“配置 FTP 协议策略”对话框中，取消选中“只读”复选框，如图 16-114 所示。





图 16-113 配置 FTP

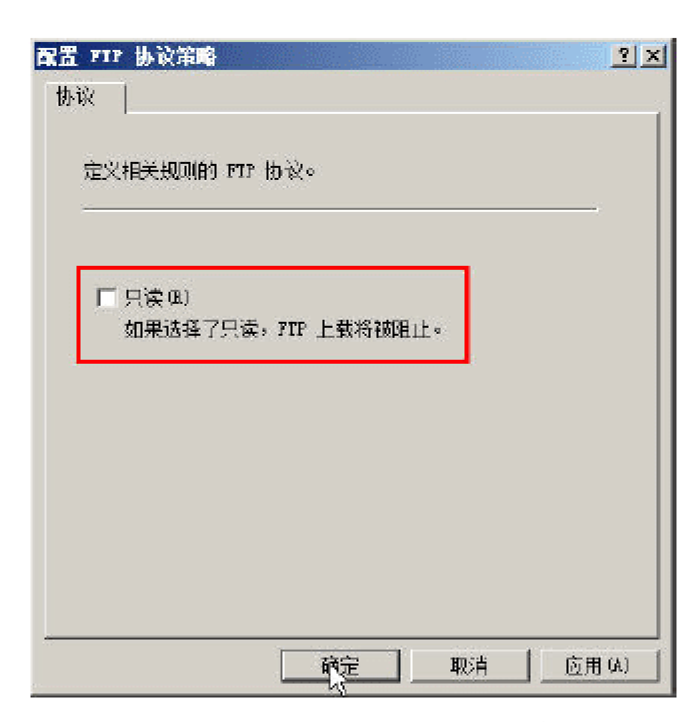


图 16-114 取消只读

10. 访问规则 6 的创建

访问规则 6 的要求是：允许其他网段在周一到周五的 8:00～11:00、14:00～17:00，以“HTTP、FTP、SMTP 与 POP3 协议”访问“外部”，在其他时间以“所有协议”访问“外部”。实际上，这是两个规则。

因为这是系统中的最后一个规则，所以，对于规则定义中的“其他网段”，可以通过添加“计算机集”，依次添加这些网段；也可以用“内部”来代替，因为前面的规则已经匹配，剩下的自然就包括“其他网段”了。在此通过添加“计算机集”的方式来实现，这样可以让规则更具体。

另外，还可以复制系统中的最后一个规则“允许所有用户访问 Web”，并在此规则的基础上修改，也可以使用新建规则向导创建。在此通过“复制”与修改的方式实现，主要步骤如下。

01 用鼠标右击“允许所有用户访问 Web”访问规则，在弹出的快捷菜单中选择“复制”命令，如图 16-115 所示。

02 然后再单击鼠标右键，在弹出的快捷菜单中选择“粘贴”命令，如图 16-116 所示。



图 16-115 复制

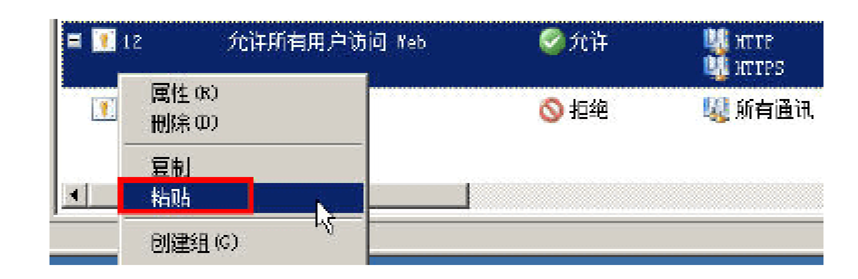


图 16-116 粘贴

03 粘贴之后，会出现两条功能相同的策略，只是名称略有区别，如图 16-117 所示。



图 16-117 复制后的策略

我们将依次修改这两条策略，主要步骤如下。

01 用鼠标双击“允许所有用户访问 Web（1）”这条策略，在“常规”选项卡中，修改名

称为“允许其他网段在工作时间上网”，并且在“描述”文本框中输入详细的规则信息（可以根据需要选择是否添加），如图 16-118 所示。

02 在“协议”选项卡中，添加“FTP、HTTP、HTTPS、POP3、SMTP”协议，如图 16-119 所示。

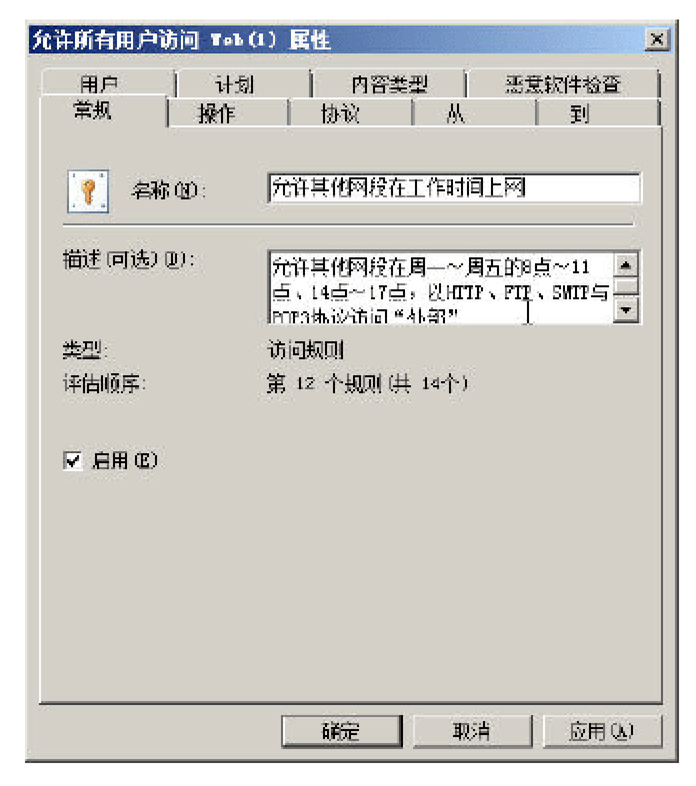


图 16-118　修改名称

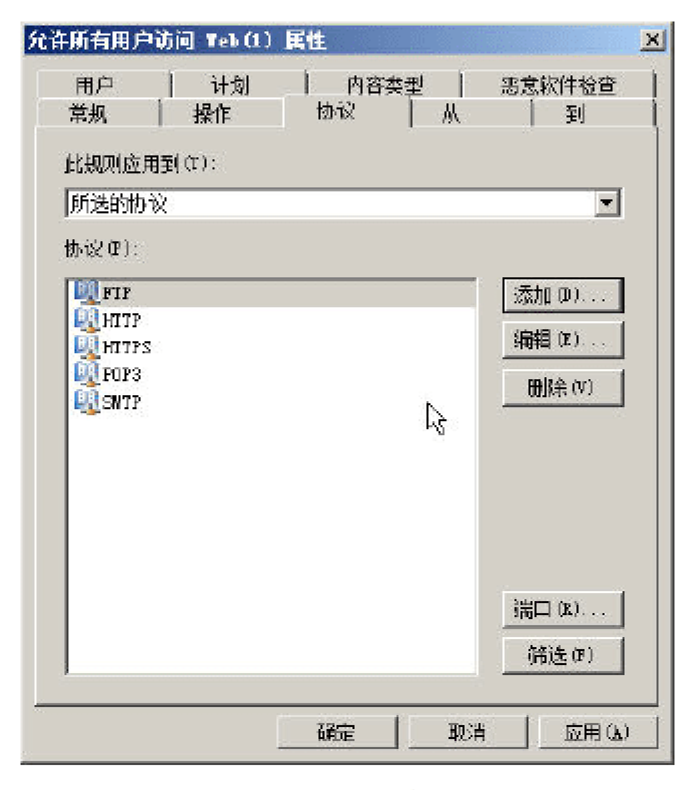


图 16-119　添加协议

03 在“从”选项卡中，选中“内部”，单击“删除”按钮，然后单击“添加”按钮，如图 16-120 所示。在“添加网络实体”对话框中，新建“计算机集”，如图 16-121 所示。

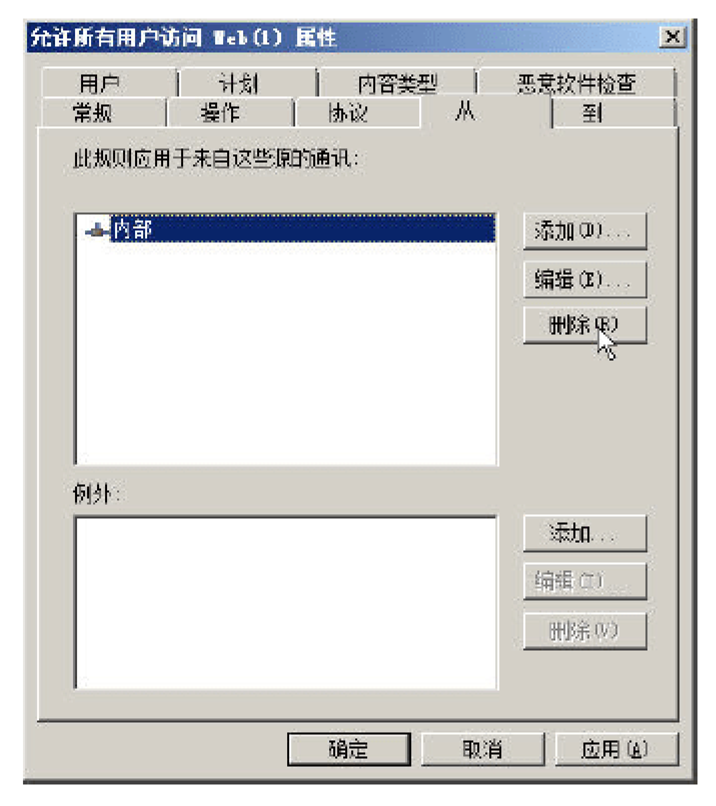


图 16-120　删除“内部”



图 16-121　新建计算机集

04 在“新建计算机集规则元素”对话框中，分别添加名为“VLAN11-15”、地址范围为 192.168.1.0-192.168.5.255 的“子网”，名称为 VLAN17、IP 地址为 192.168.7.0/24 的“子网”，以及名称为“VALN19-20”、地址范围为 192.168.9.0-192.168.10.255 的“子网”，如图 16-122 所示。然后将“其他网段”添加到“从”选项卡中，如图 16-123 所示。

05 在“计划”选项卡，添加名为“上班时间”的计划，时间为周一到周五的 8:00 ~ 12:00、14:00 ~ 17:00，如图 16-124 所示。设置完成后，这条规则创建完成，单击“确定”按钮。

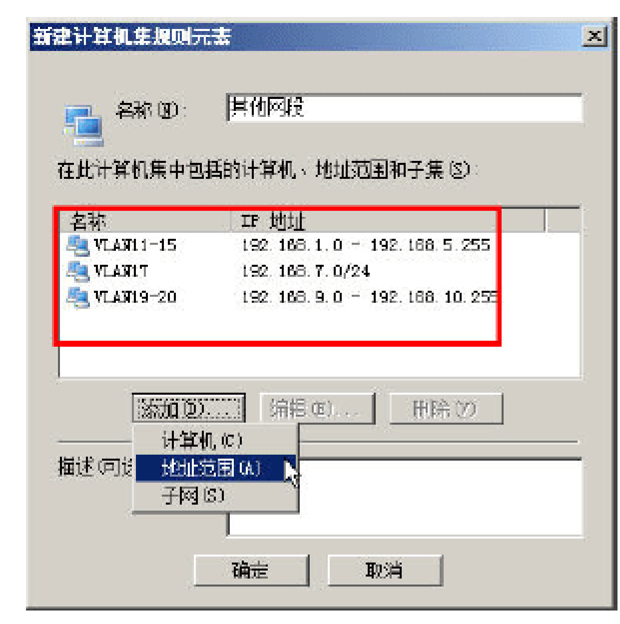


图 16-122　添加计算机集

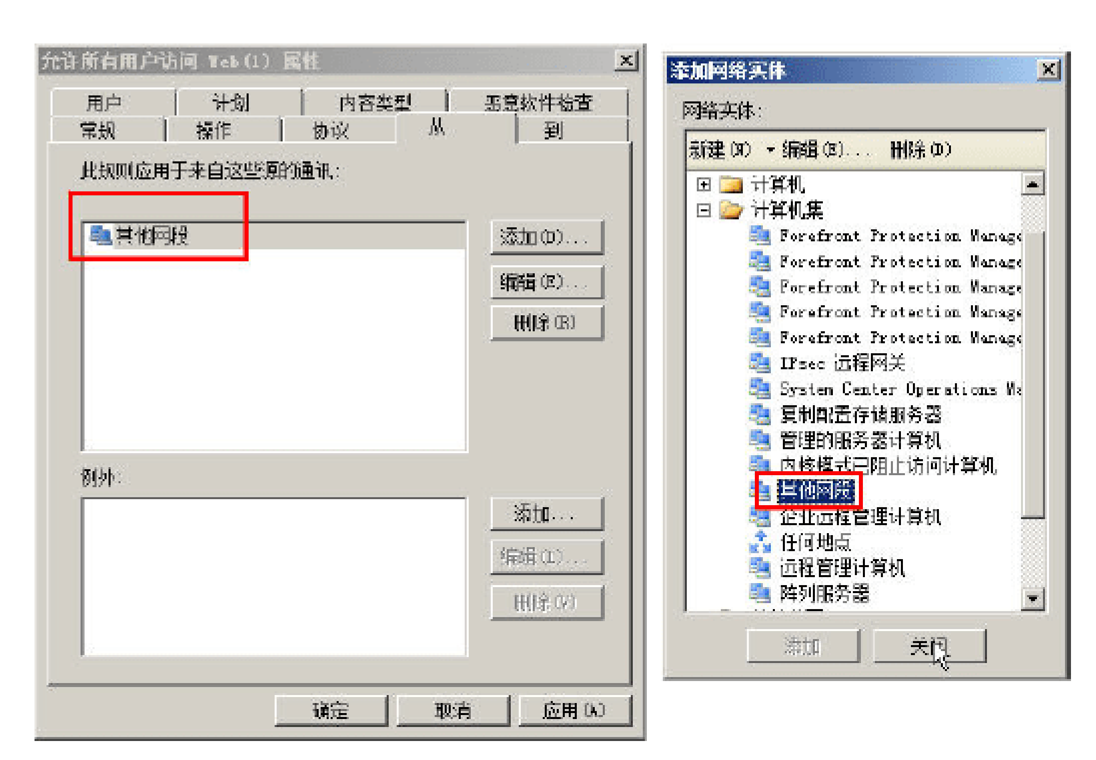


图 16-123　添加其他网段　　　　图 16-124　添加计划

11. 检查策略顺序并应用更改

做完上述策略之后，根据事先的规则，检查策略及策略顺序是否符合我们的需求，可以通过选中策略并单击工具栏上的“↑”“↓”按钮进行调整。在调整之前，先选中最后两条策略，单击鼠标右键，在弹出的快捷菜单中选择“取消组合”命令，然后再进行调整，如图 16-125 所示。



图 16-125　取消组合

说 明

组合是 Forefront TMG 中新增加的功能，使用此功能可以将多个不同的策略“组合”在一起，进行分组管理。这样在有多条策略时，可以通过展开（单击工具栏上的＋）或者折叠分组（单击工具栏上的－），让管理界面更加简洁。

最后，通过单击“应用”按钮，让设置生效。在 Forefront TMG 中，增加了“配置更改描述”的对话框，在此可以输入当前配置更改的原因，如图 16-126 所示。如果以后不想使用这个功能，可以选中“不再显示此提示”复选框。

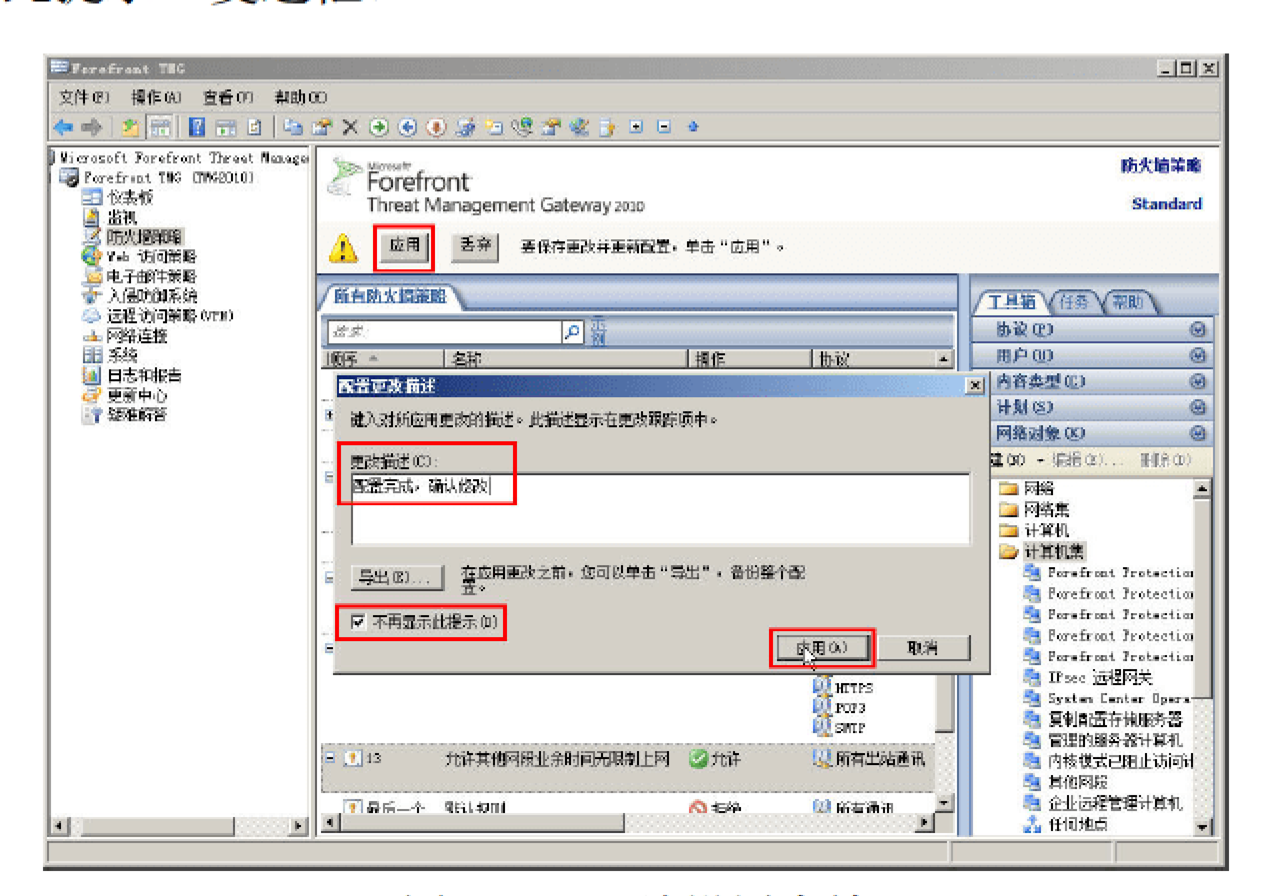


图 16-126　让设置生效

16.4.3 系统策略

在安装 Forefront TMG 时，将配置一组预定义规则（称为系统策略规则），这些规则默认是不会显示的。如果要显示系统策略，在 Forefront TMG 控制台中的“查看”菜单中，选择“显示系统策略规则”命令即可，如图 16-127 所示。

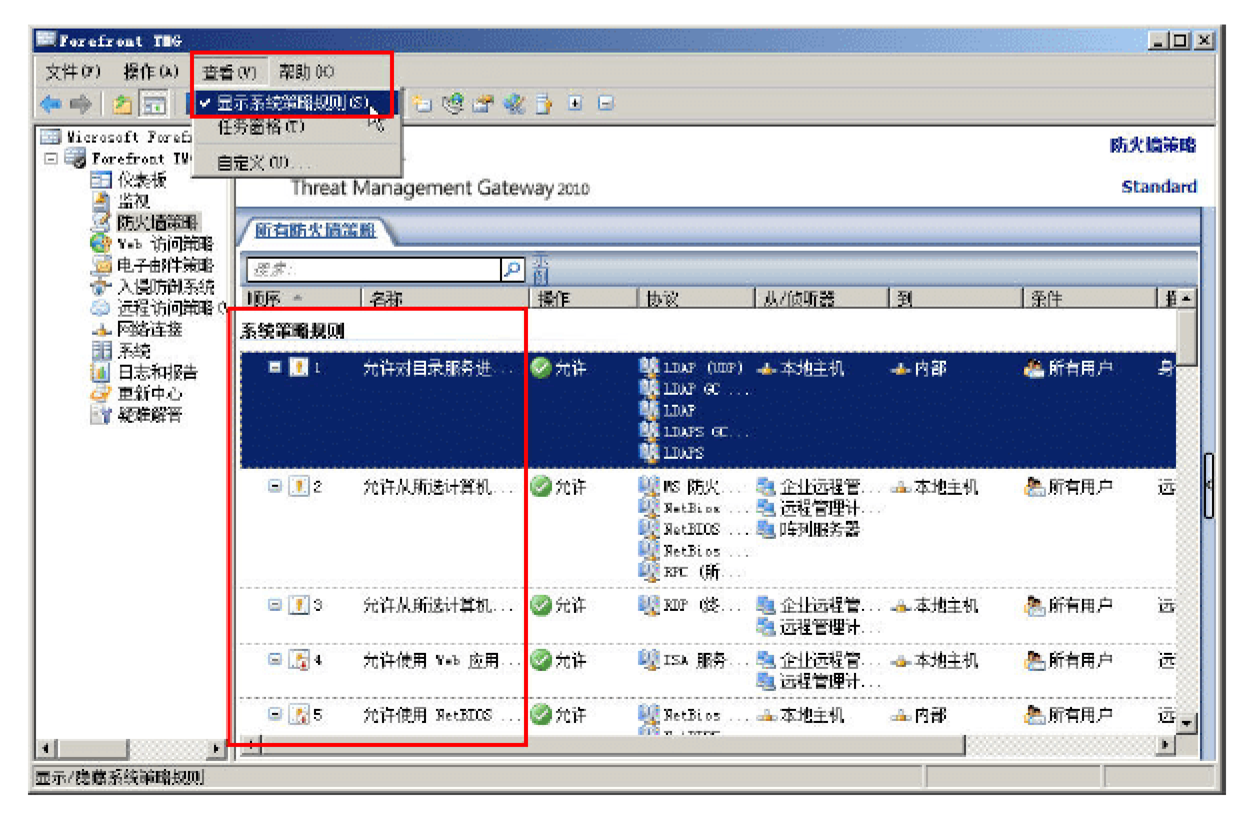


图 16-127　显示系统策略规则

在系统策略规则中，可以启用或禁用单独的规则，并修改规则目标，但不能删除现有规则或创建新规则。

说 明

一般情况下，不要修改或禁用系统规则。改变系统规则，有可能引起安全或者网络问题。只有在确实需要时，才可以“暂时”修改系统规则，当所做工作完成后，再次恢复系统策略。

例如，在 Forefront TMG 的计算机中，安装了“Internet 信息服务”并且在通过“企业证书服务器”申请证书的时候，会出现“RPC 服务器不可用”的错误提示，如图 16-128 所示。这个时候，就需要修改第 22 条系统策略（用鼠标右击“允许从 Forefront TMG 到受信任的服务器的 RPC”，从弹出的快捷菜单中选择“编辑系统策略”命令），并且取消选中“强制严格符合 RPC”复选框，如图 16-129 所示，才能解决这个错误。

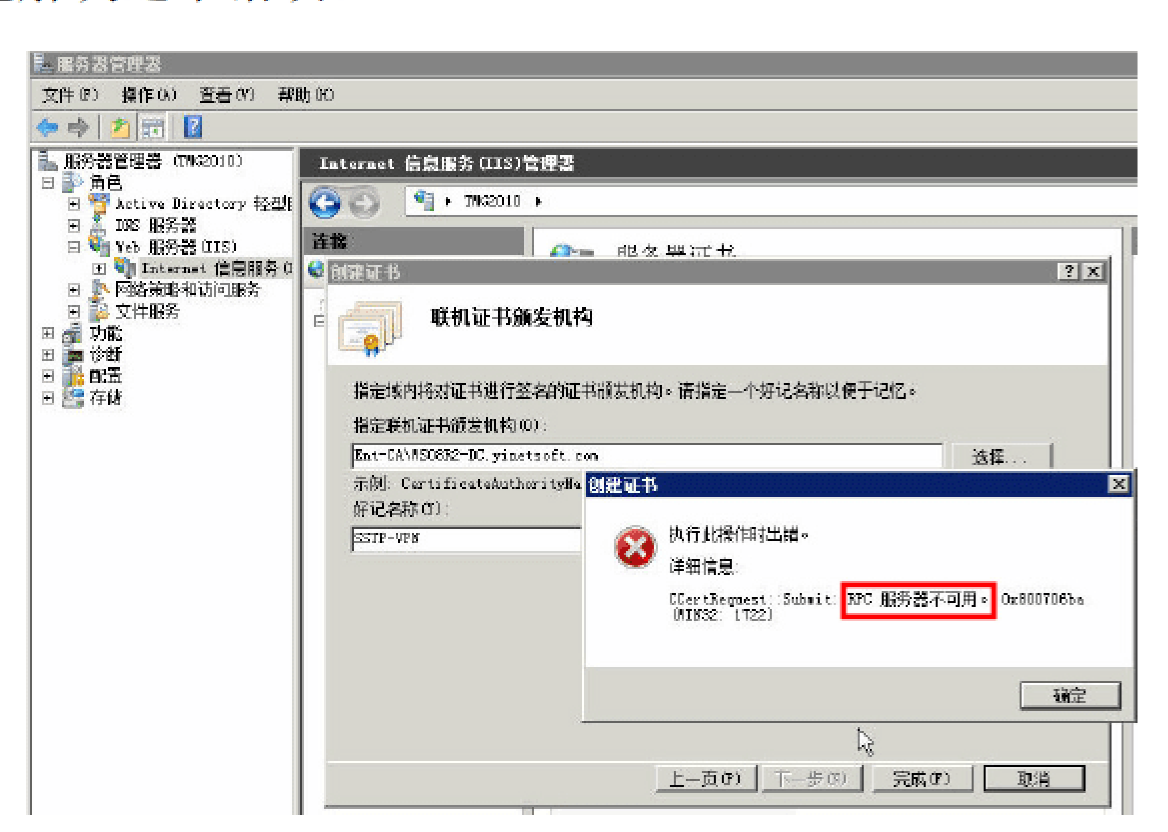


图 16-128　提示 RPC 服务不可用

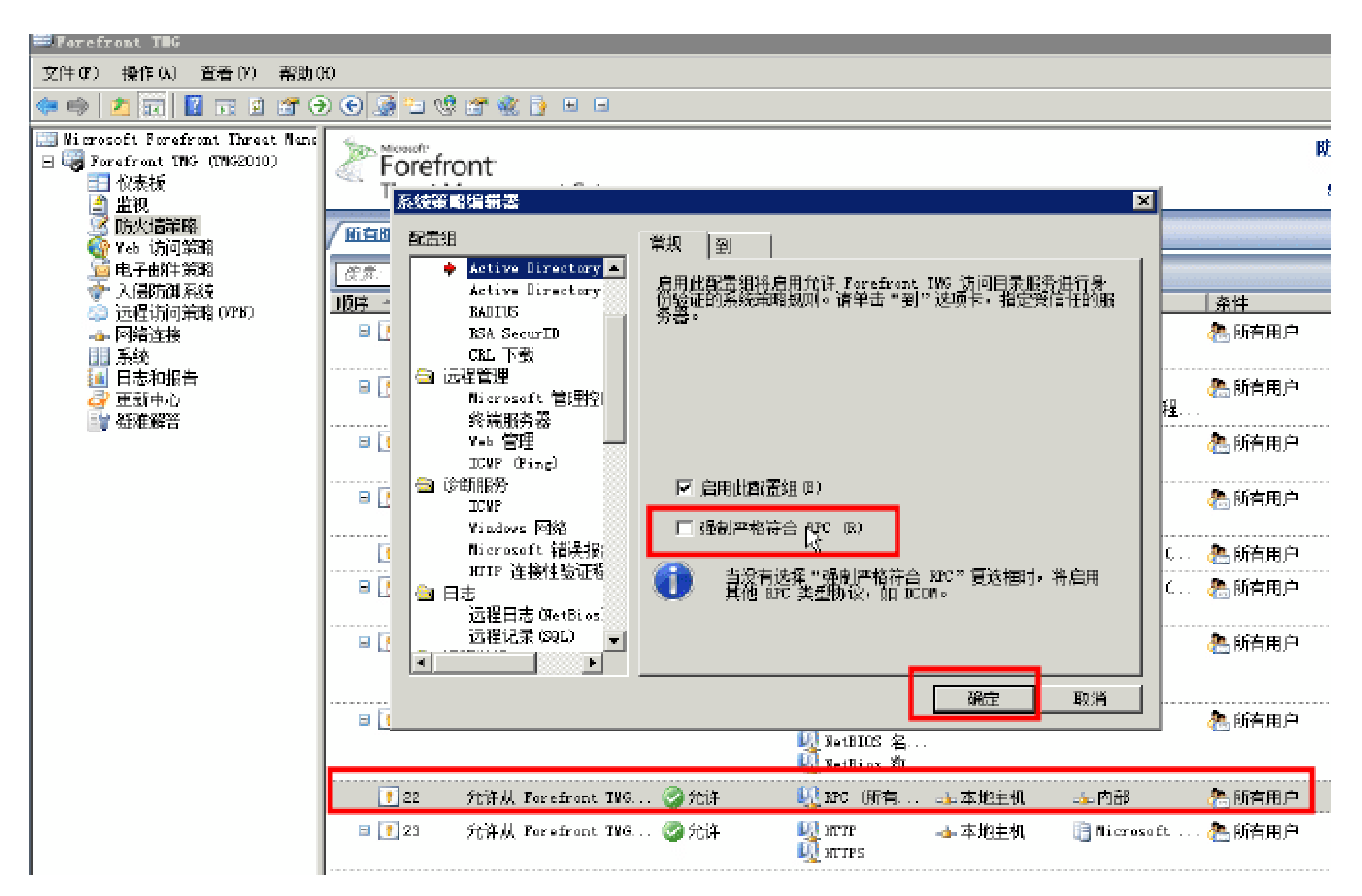


图 16-129　取消严格 RPC 检查

在申请证书之后，恢复系统策略。

16.5　组建基于 PPTP 与 L2TP 的 VPN 网络

在“远程访问策略”中，可以将 Forefront TMG 配置成 VPN 服务器（允许远程用户通过 Internet，以 VPN 方式连接到 Forefront TMG 所保护的内网），或者将 Forefront TMG 配置成 VPN 路由器（连接多个远程的网络）。本文先介绍基于 PPTP 与 L2TP 的 VPN 网络的组建，网络拓扑如图 16-130 所示。

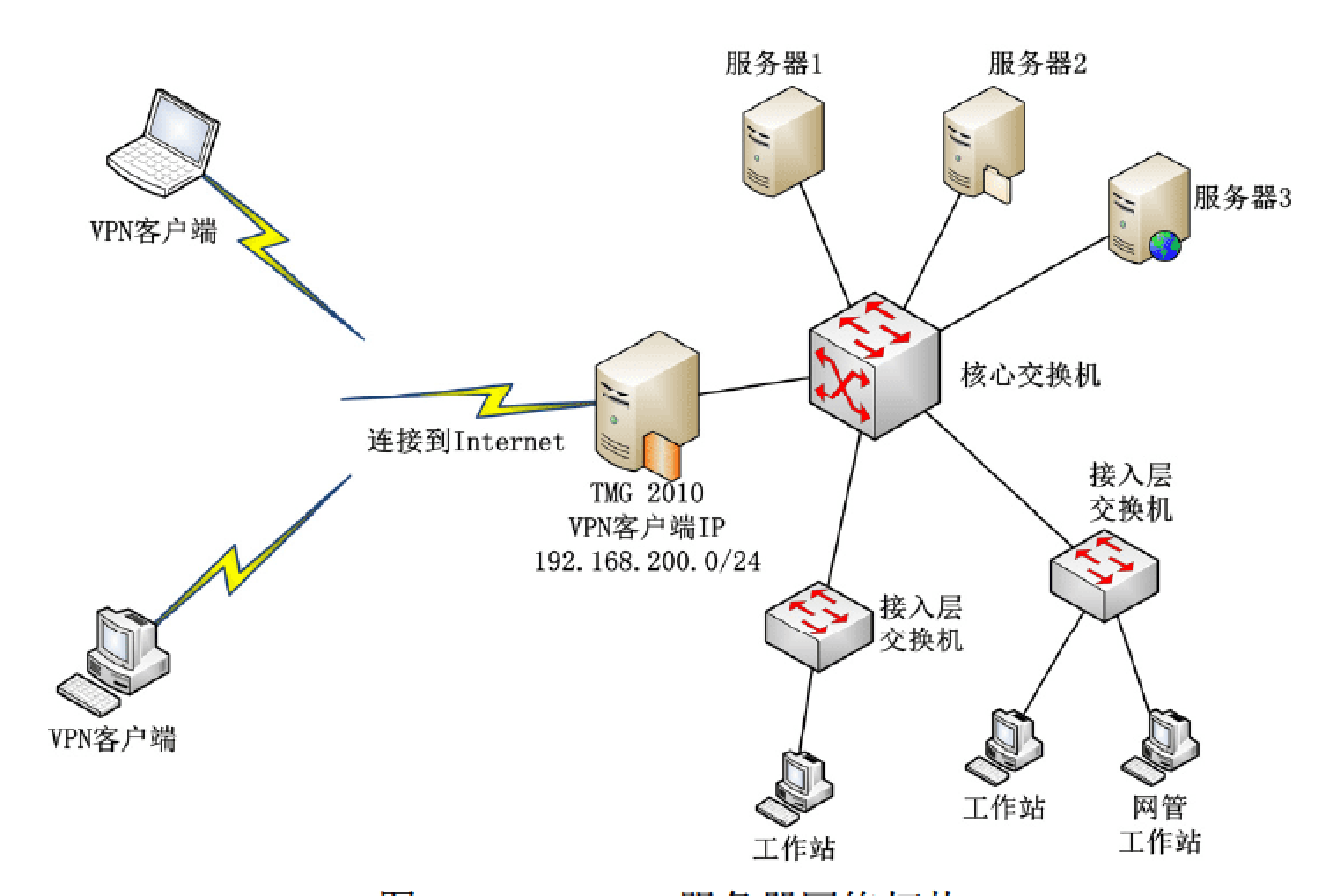


图 16-130　VPN 服务器网络拓扑

在图 16-130 中，是在前文（图 16-50）的基础上，将网络中原来的 Forefront TMG 2010 配置成 VPN 服务器，并为 Internet 用户提供 VPN 拨入的拓扑。在本案例中，为 VPN 客户端规划的 IP 地址是 192.168.200.0/24，并且允许 VPN 客户端访问“服务器 1”与“服务器 3”（以“内网”用户的身份）。接下来介绍这个案例的配置。

16.5.1 在 Forefront TMG 中启用 VPN 服务器

在 Forefront TMG 中，启用 VPN 服务的步骤如下。

01 在 Forefront TMG 管理器的“远程访问策略（VPN）”节点，单击“VPN 客户端”选项卡，在右侧的“任务”选项卡中单击“定义地址分配”链接，如图 16-131 所示。



图 16-131 定义地址分配

02 在“远程访问策略（VPN）属性”对话框中，在“地址分配”选项卡中，定义给 VPN 客户端分配 IP 地址的方式。如果网络中存在 DHCP 服务器（此 DHCP 服务器与 VPN 服务器不能在同一主机上），可以使用 DHCP 服务器分配。如果网络中没有 DHCP 服务器，或者不想使用 DHCP 服务器分配的地址，可以选中“静态地址池”单选按钮，并且单击“添加”按钮，在弹出的“服务器 IP 地址范围属性”对话框中，输入 VPN 客户端的地址范围。在本例中，为 192.168.200.0～192.168.200.255，如图 16-132 所示。

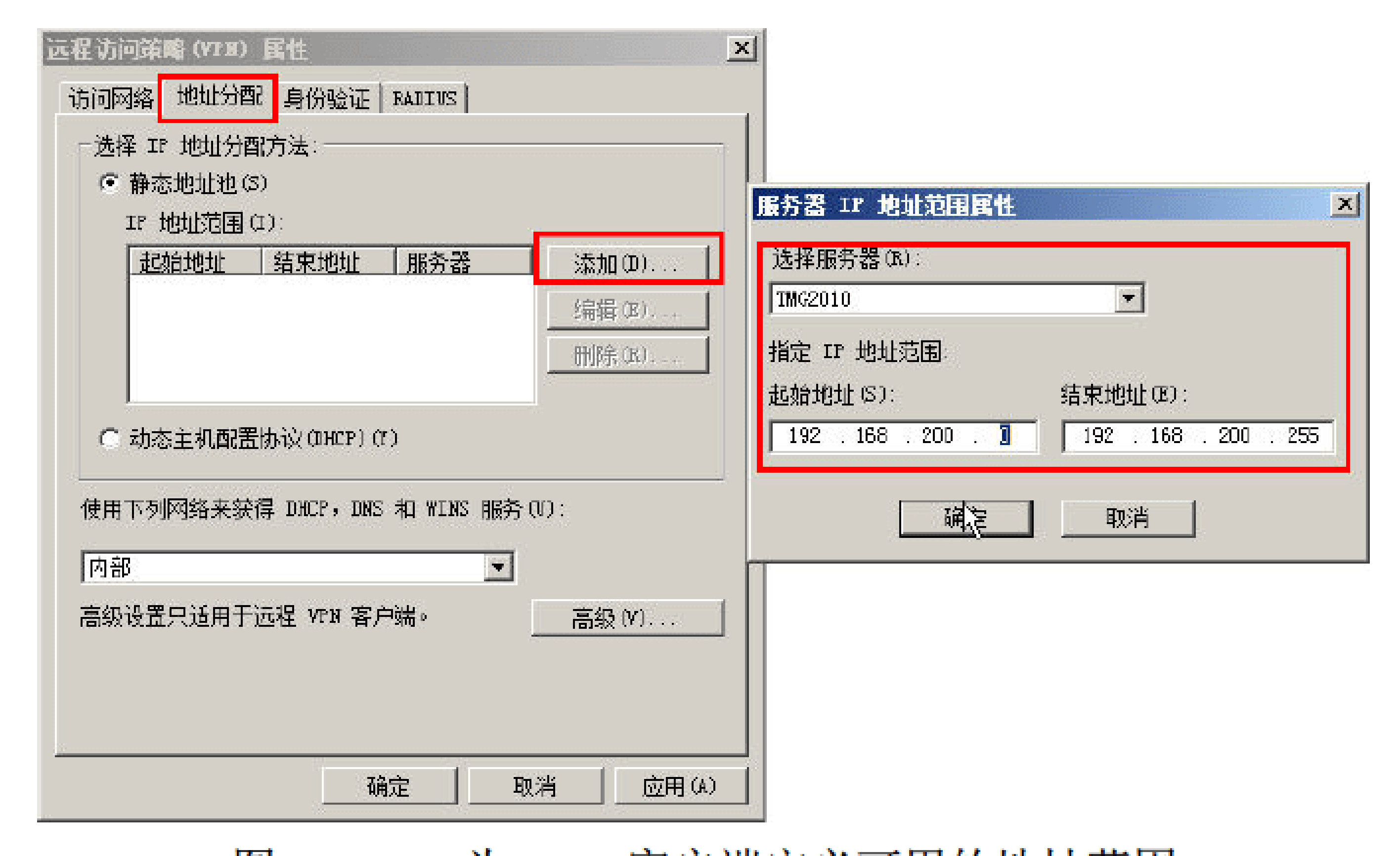


图 16-132 为 VPN 客户端定义可用的地址范围

03 在“身份验证”选项卡中，选择 VPN 客户端与 Forefront TMG 的 VPN 服务器连接时使用的身份验证方法。通常情况下，选择默认值即可，如图 16-133 所示。

04 在“RADIUS”选项卡中，指定是否启用 RADIUS 服务器对 VPN 客户进行身份验证。默认情况下，使用 Forefront TMG 这台“本地计算机”进行身份验证，所以不需要设置。如图 16-134

所示。当然，如果要使用网络中的其他 RADIUS 服务器进行身份验证，可以选中“使用 RADIUS 进行身份验证”复选框并且单击“RADIUS 服务器”按钮，添加 RADIUS 服务器的地址及身份验证消息。

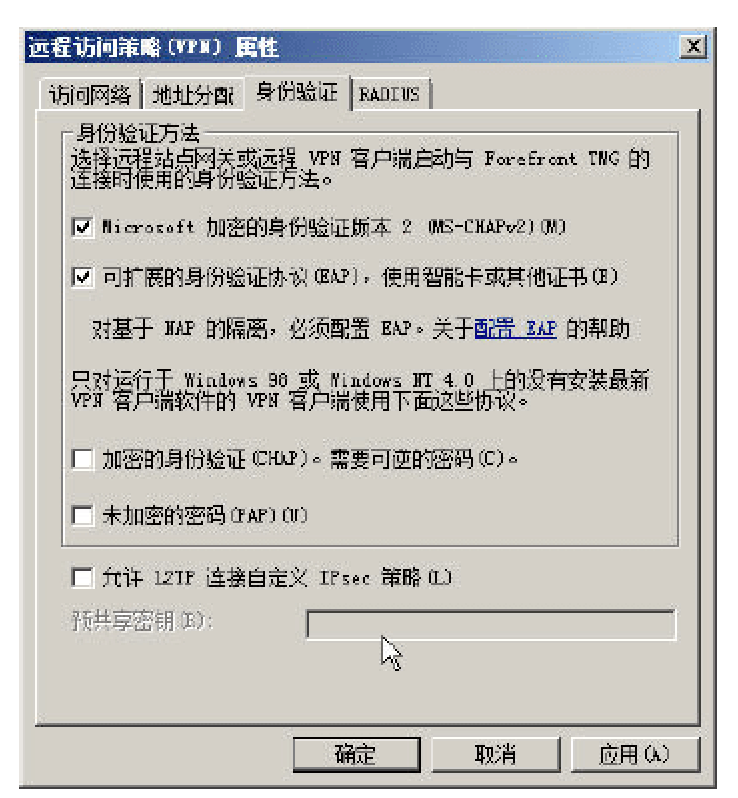


图 16-133　身份验证方法

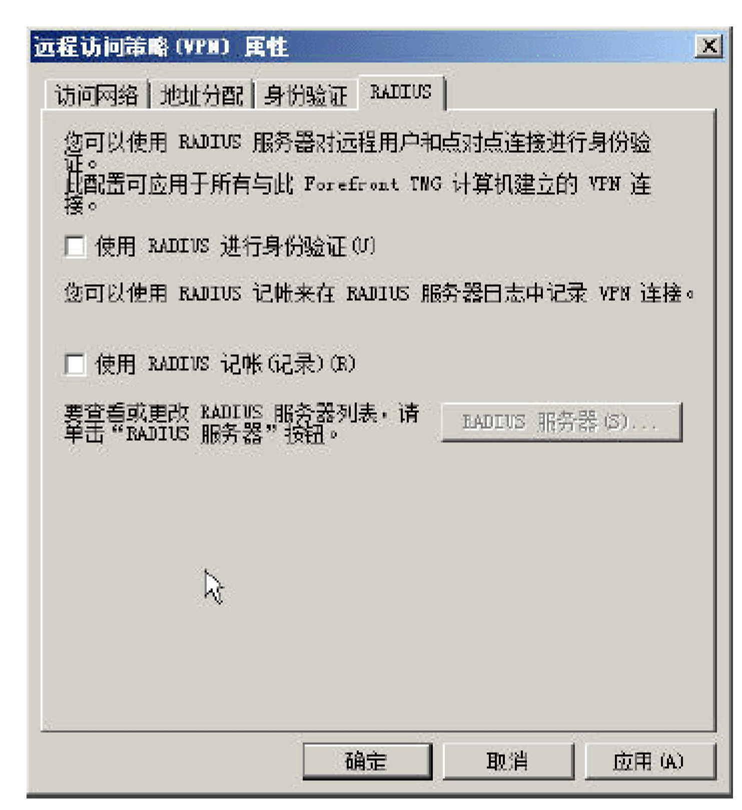


图 16-134　是否选择 RADIUS 进行身份验证

05 在“访问网络”选项卡中，选择对 VPN 客户端进行侦听的网络，默认情况下是“外部”，即 VPN 服务器只对 Internet 用户生效，如图 16-135 所示。设置之后，单击“确定”按钮，返回 Forefront TMG 控制台。



说 明

如果在内网也需要 VPN 服务器，可以在“访问网络”选项卡中选中“内部”复选框，这样，VPN 客户端可以通过拨叫 Forefront TMG 内网的 IP 地址，来呼叫 VPN 服务器。

06 在 Forefront TMG 控制台右侧窗格的“任务”选项卡中，单击“配置 VPN 客户端访问”链接，在弹出的“VPN 客户端 属性”对话框中，在“协议”选项卡中，选择远程访问连接可用的隧道协议，如图 16-136 所示。在默认情况下，Forefront TMG 的 VPN 服务器选择 PPTP 与 L2TP/IPsec。

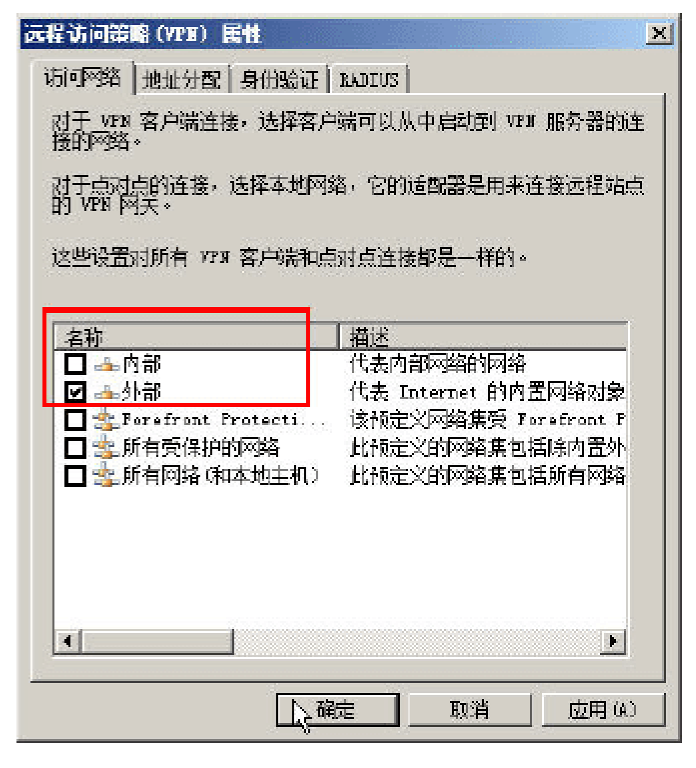


图 16-135　访问网络

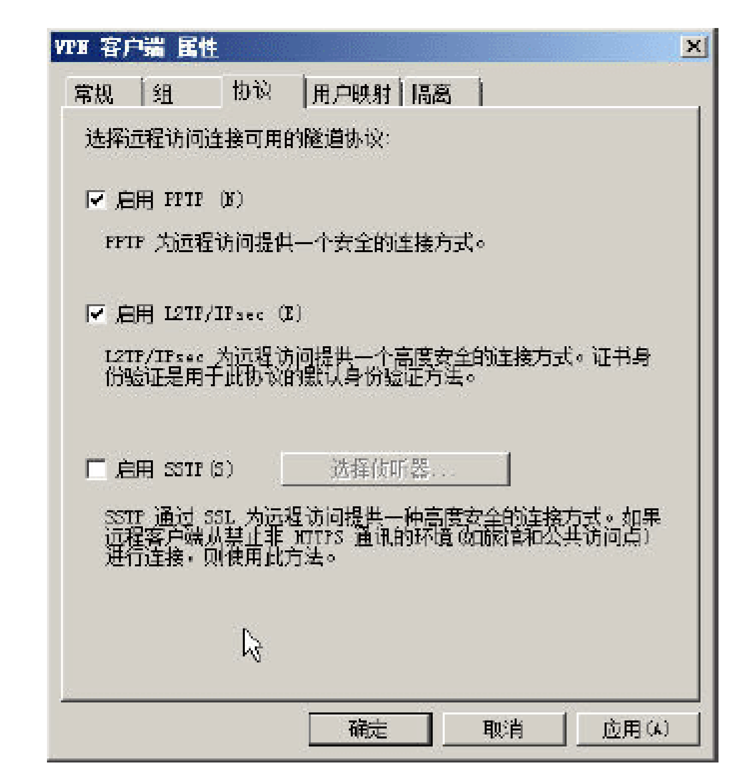
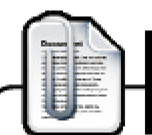


图 16-136　协议



说 明

如果要使用 SSTP 协议，需要为 Forefront TMG 申请一个“服务器证书”并安装在“本地计算机存储”中。在本文的 16.7 节将介绍这方面内容。

07 在“常规”选项卡中，选中“启用 VPN 客户端访问”复选框，并且设置“允许的最大 VPN 客户端数量”，在此设置为 200，如图 16-137 所示。设置完成后，单击“确定”按钮。



说 明

在指定最大 VPN 客户端数量时，要保证有足够的 VPN 客户端地址（在图 16-132 中设置），如果可用的 VPN 客户端地址不够，将会弹出错误的消息并不能继续，如图 16-138 所示。

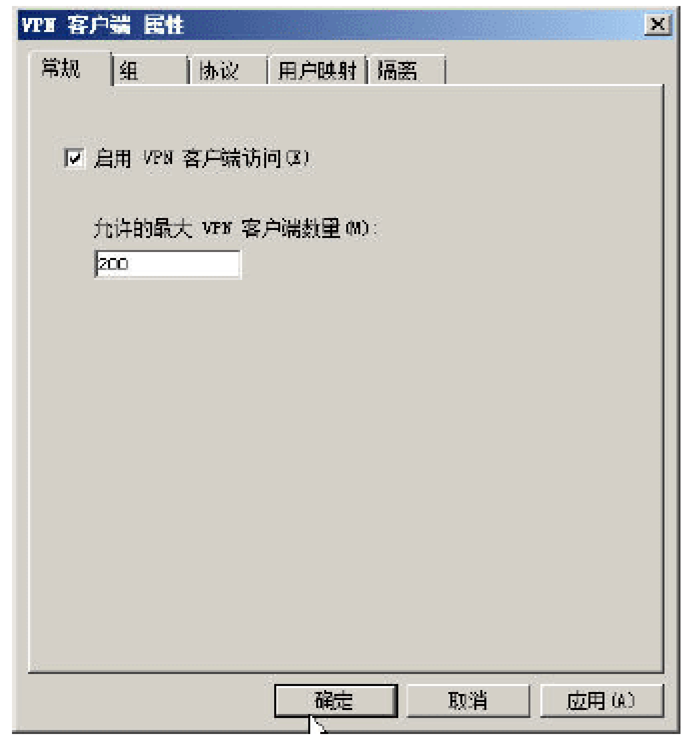


图 16-137 启用 VPN 客户端访问

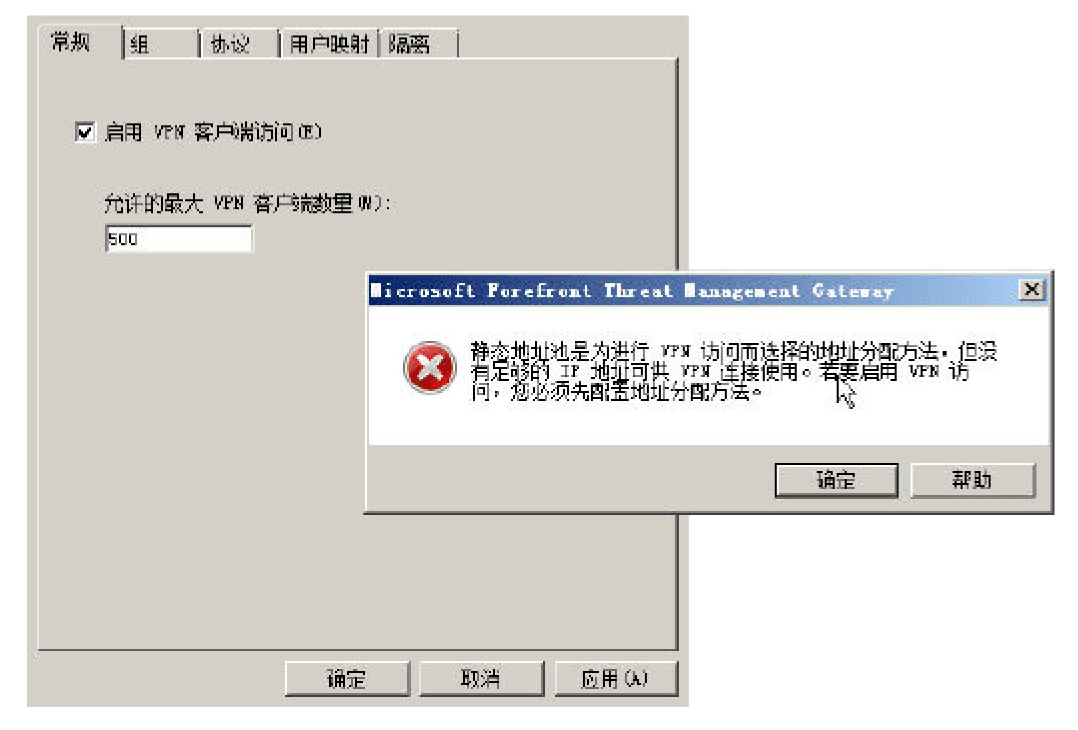


图 16-138 IP 地址不够

08 返回到 Forefront TMG 控制台，单击“应用”按钮，让设置生效。同时，最好在“配置更改描述”对话框中，写清配置更改的原因，如图 16-139 所示。

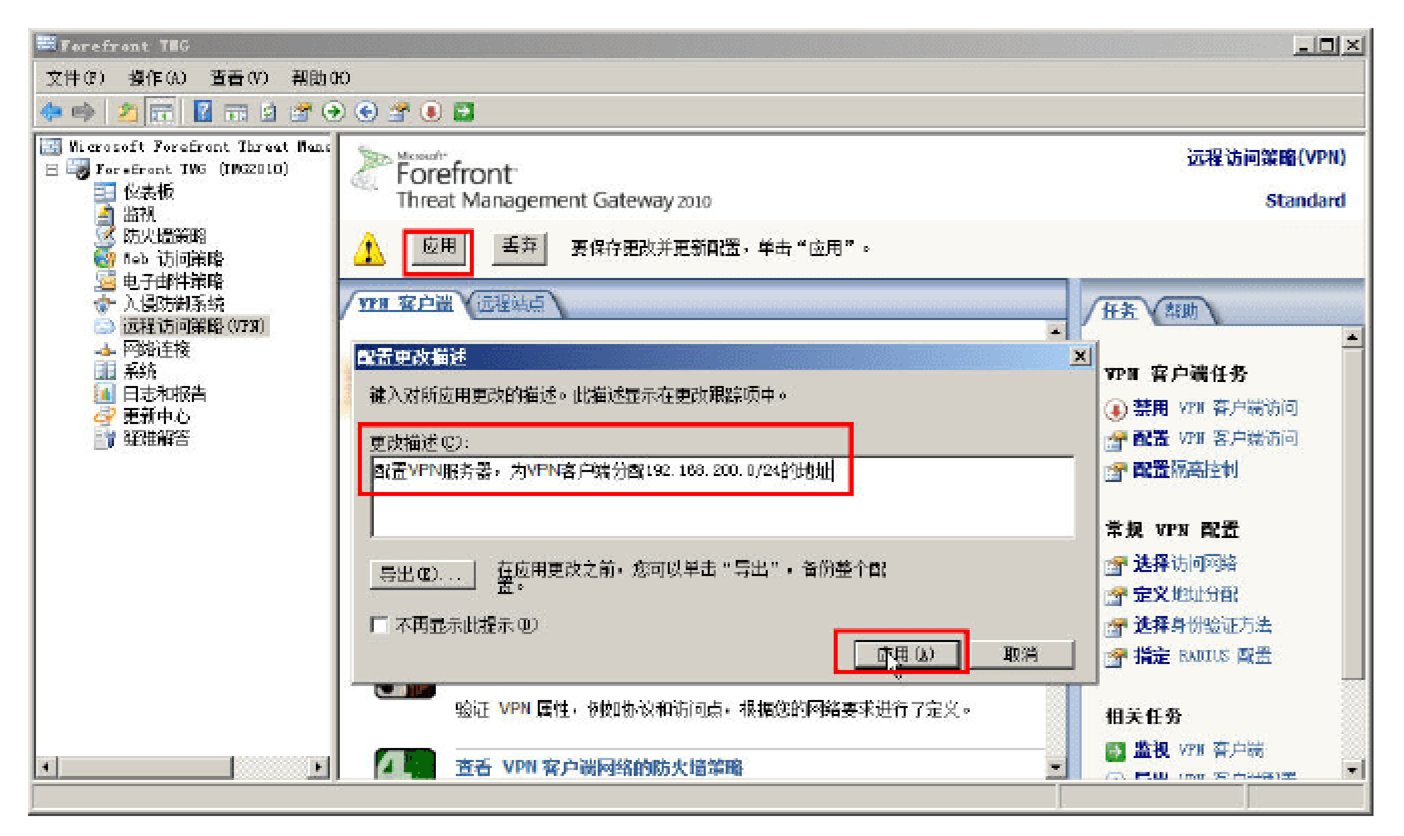


图 16-139 应用

在配置完 VPN 服务器后，还需要在“防火墙策略”中，新建一条规则，允许 VPN 客户端访问服务器 1、服务器 3。主要步骤如下。

01 访问规则名称定义为“允许 VPN 客户端访问服务器 1、服务器 3”，如图 16-140 所示。

02 规则操作为“允许”。

03 所选协议为“所有出站通信”。

04 在“访问规则源”对话框中，添加“VPN 客户端”与“被隔离的 VPN 客户端”，如图 16-141 所示。

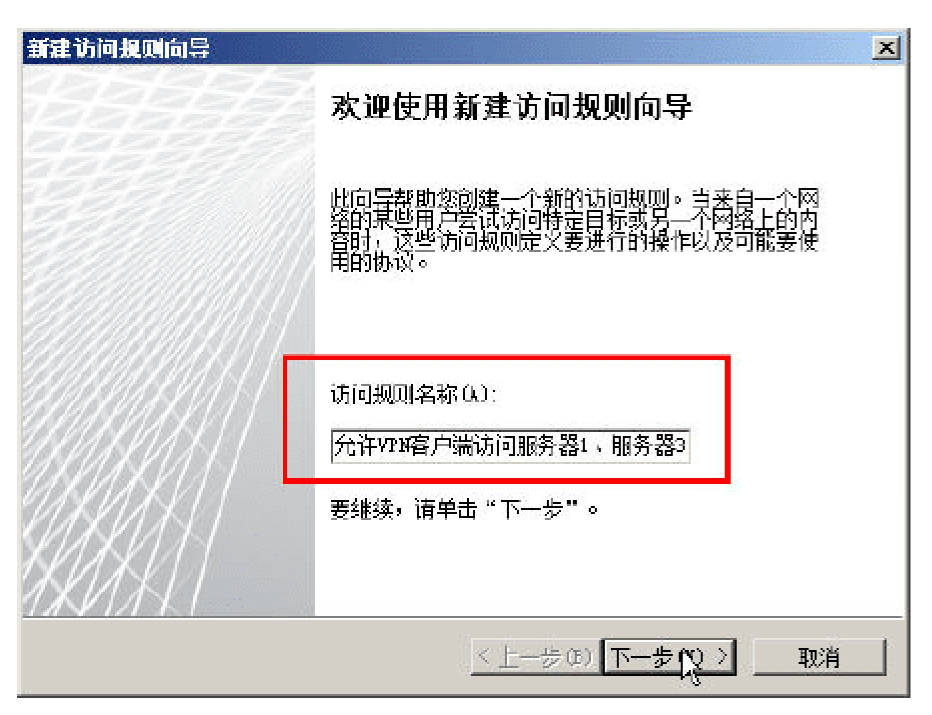



图 16-140　访问规则

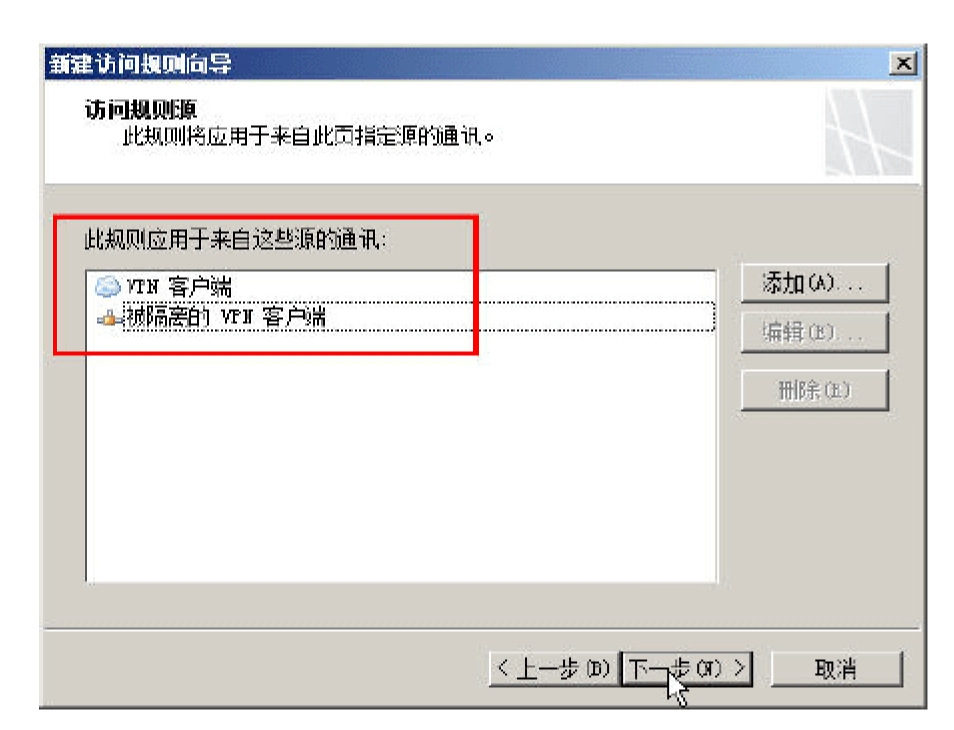


图 16-141　访问规则源

05 在"访问规则目标"对话框中，添加"服务器 1"与"服务器 3"，如图 16-142 所示。

06 其他选择默认值。添加完成后，单击"应用"按钮，让设置生效。

在第一次配置 VPN 服务器的时候，需要重新启动计算机。重新启动 Forefront TMG 的计算机，如图 16-143 所示。

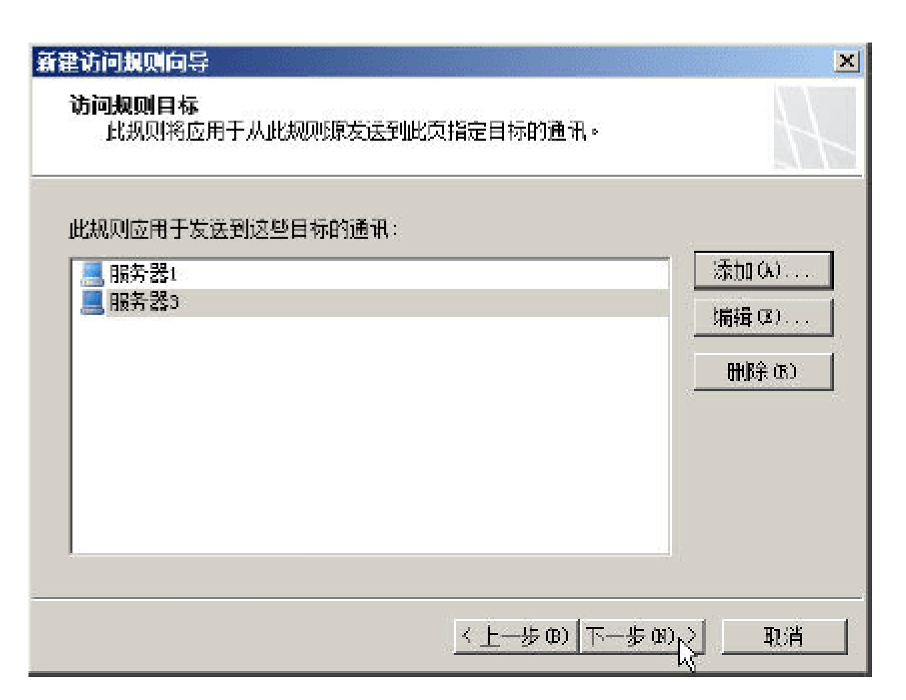


图 16-142　访问规则目标

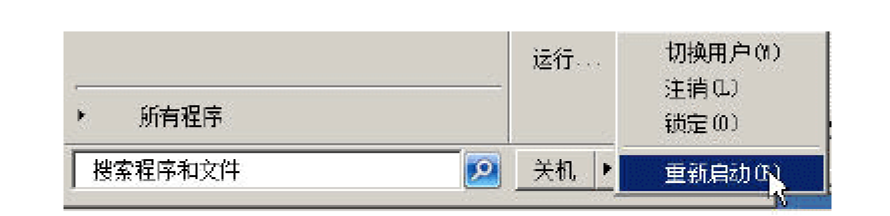


图 16-143　重新启动 Forefront TMG

16.5.2　用户管理与设置

再次进入 Forefront TMG 后，需要为 VPN 客户端创建用户。操作步骤如下。

01 进入"服务器管理器"，定位到"配置→本地用户和组→用户"节，在右侧空白窗格中单击鼠标右键，从弹出的快捷菜单中选择"新用户"命令，如图 16-144 所示。

02 在弹出的"新用户"对话框中输入"用户名"、"密码"，并取消选中"用户下次登录时须更改密码"对话框，然后单击"创建"按钮。创建用户完成后，可以继续创建用户，也可以单击"关闭"按钮，退出用户创建，如图 16-145 所示。在本例中，创建的用户名是 vpn，密码是 a1b2c3D4，密码区分大小写。

03 双击新创建的用户，在"vpn 属性"对话框的"拨入"选项卡中，选中"允许访问"单选按钮，如图 16-146 所示，然后单击"确定"按钮。此时，所有的远程 VPN 客户机可以使用此用户名拨入并可自动获取地址，获取的地址为图 16-132 中设置的地址范围。如果想给每一个 VPN 接入用户创建一个用户名，并且想给接入的 VPN 用户分配固定的 IP 地址，可选中"分配静态 IP 地址"复选框，并单击"静态 IP 地址"按钮，为用户指定固定的 IPv4 或 IPv6 地址，如图 16-147 所示。

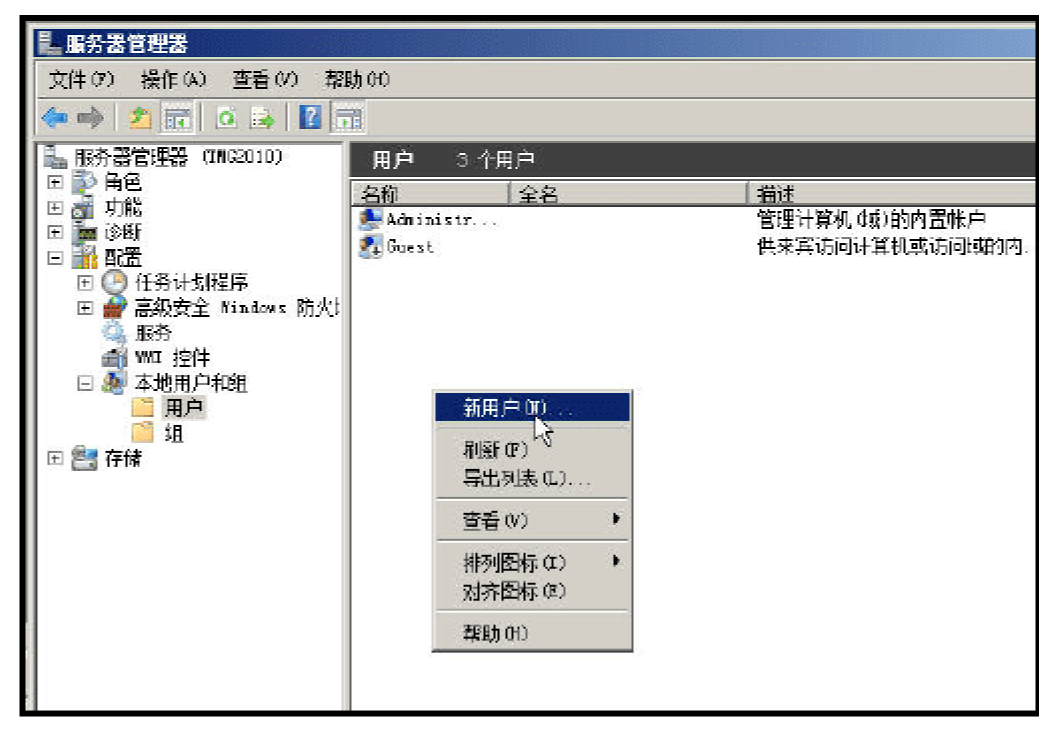




图 16-144　新建一个用户



图 16-145　创建用户

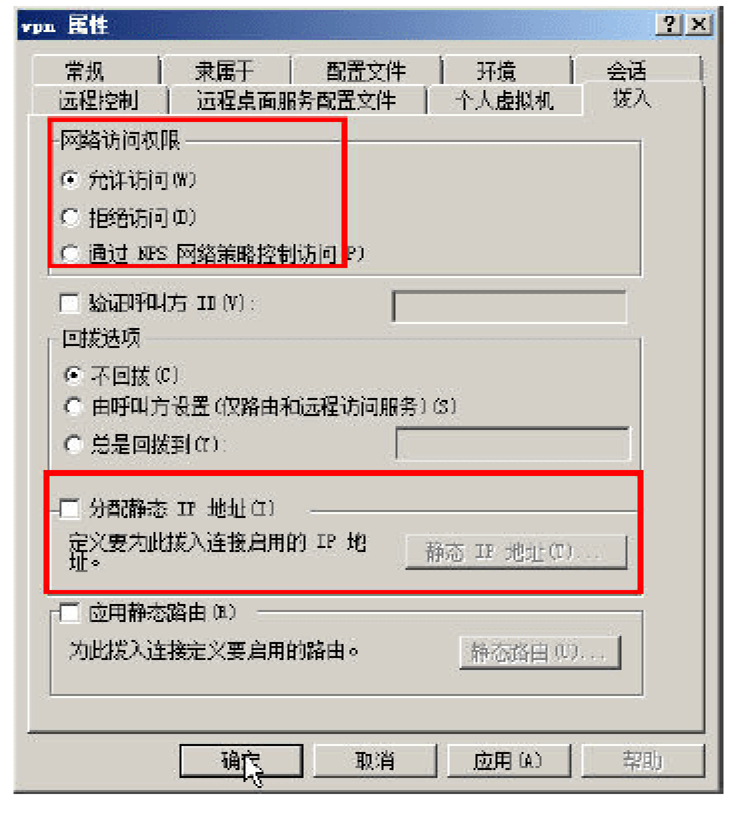


图 16-146　允许远程访问权限

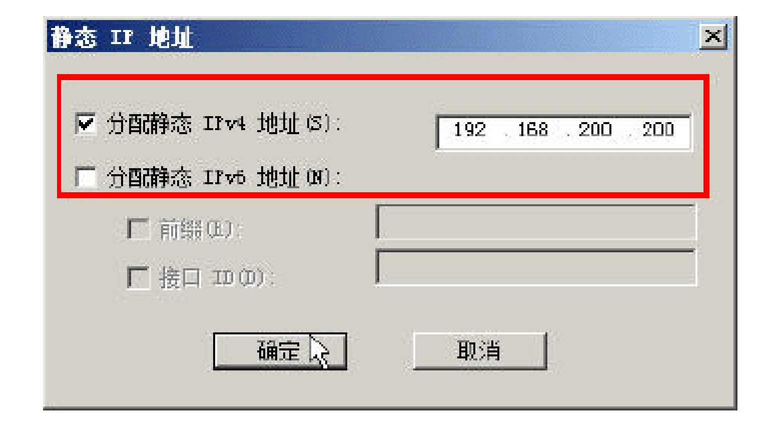


图 16-147　为 VPN 用户指定固定地址

为 VPN 用户分配了固定 IP 地址后，当此用户拨入，系统会为该用户分配图 16-147 中“分配静态 IPv4 地址”后指定的地址。如果该地址已经被使用，则系统会为用户分配一个可用的其他地址。

04 设置之后，单击“确定”按钮返回。

16.6　配置 VPN 站点间路由

在“远程站点”选项卡中，可以配置 VPN 站点间路由，用 Forefront TMG 连接两个（或多个）内部局域网。在本节中，同样通过案例的方式进行介绍，所用网络拓扑如图 16-148 所示。

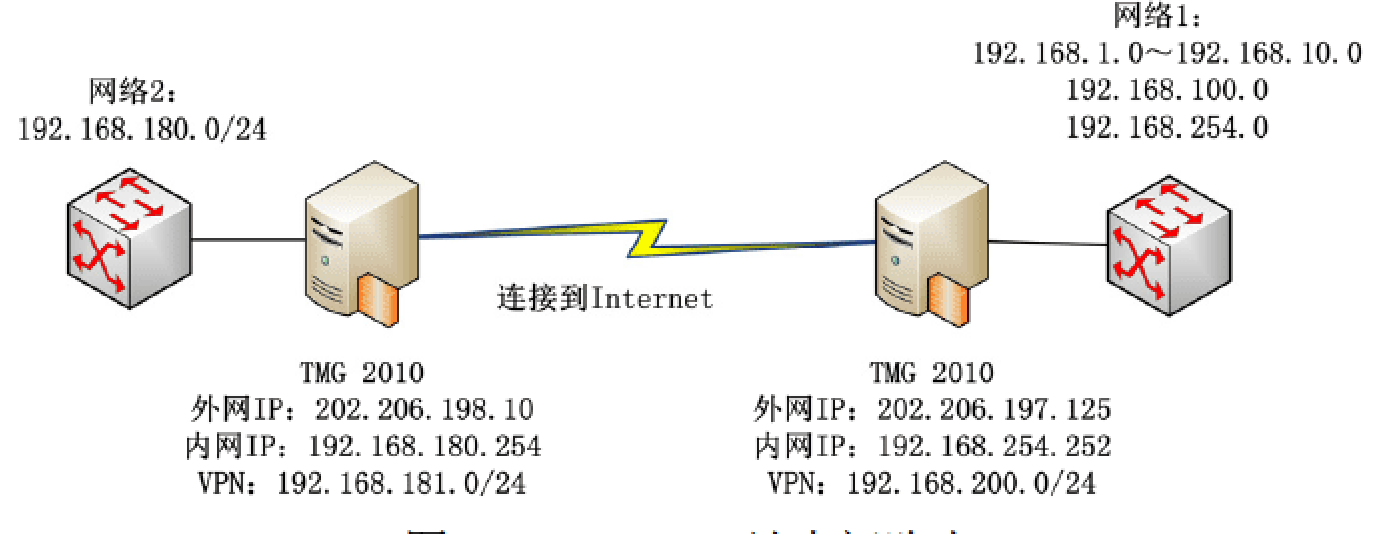


图 16-148　VPN 站点间路由

在图 16-148 中，网络 1 的内部网络是 192.168.1.0～192.168.10.0/24、192.168.100.0/24、192.168.254.0/24，Forefront TMG 的外网地址是 202.206.197.125；网络 2 的内部地址是 192.168.180.0/24，Forefront TMG 的外网地址是 202.206.198.10.

首先介绍网络 1 中，Forefront TMG 的配置，步骤如下。

01 在 Forefront TMG 的控制台中，定位到“远程访问策略 VPN”节点，单击“远程站点”选项卡，然后单击“创建 VPN 点对点连接”链接，如图 16-149 所示。

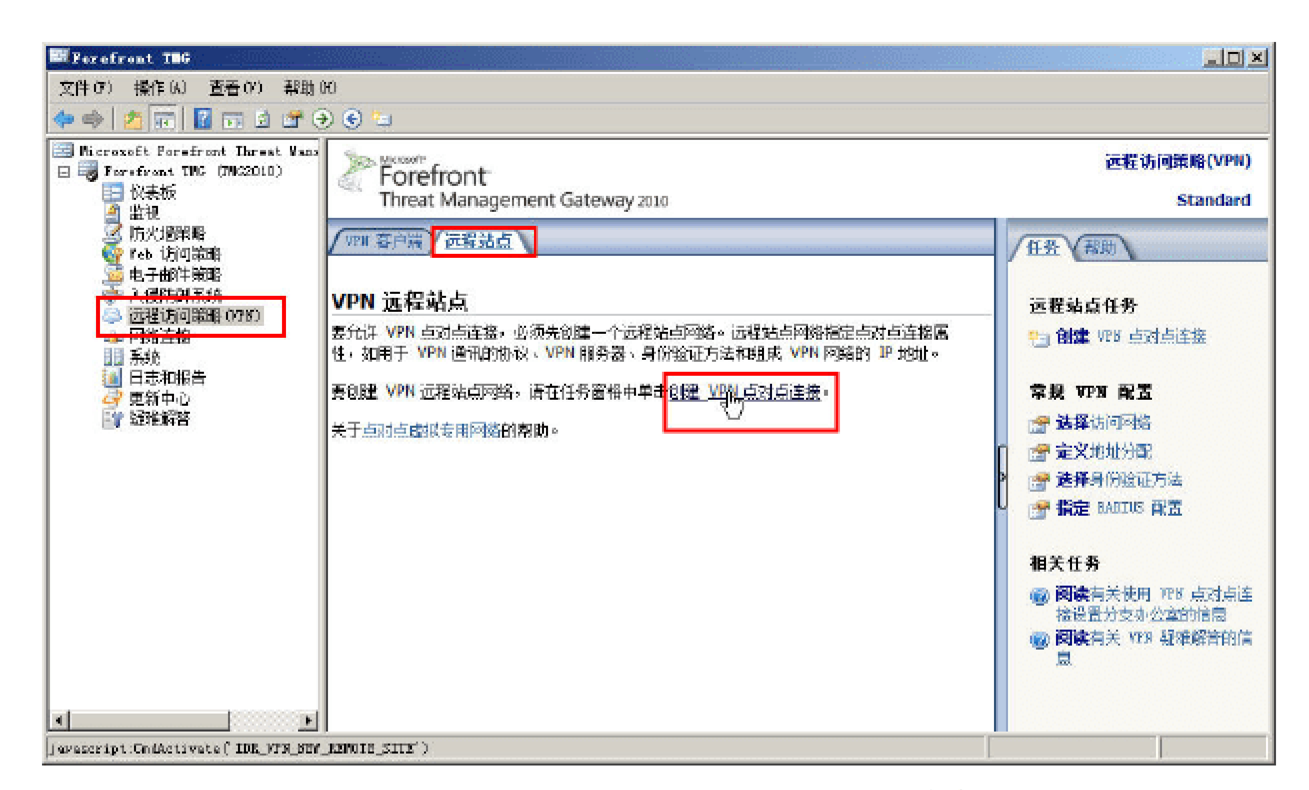


图 16-149 创建 VPN 点对点连接

02 在“欢迎使用创建 VPN 点对点连接向导”对话框中，在“点对点网络名称”文本框中，输入新创建的连接名称。在此推荐使用英文名称，本例为 RRAS，如图 16-150 所示。

03 在“VPN 协议”对话框中，选中“点对点隧道协议（PPTP）”单选按钮，如图 16-151 所示。

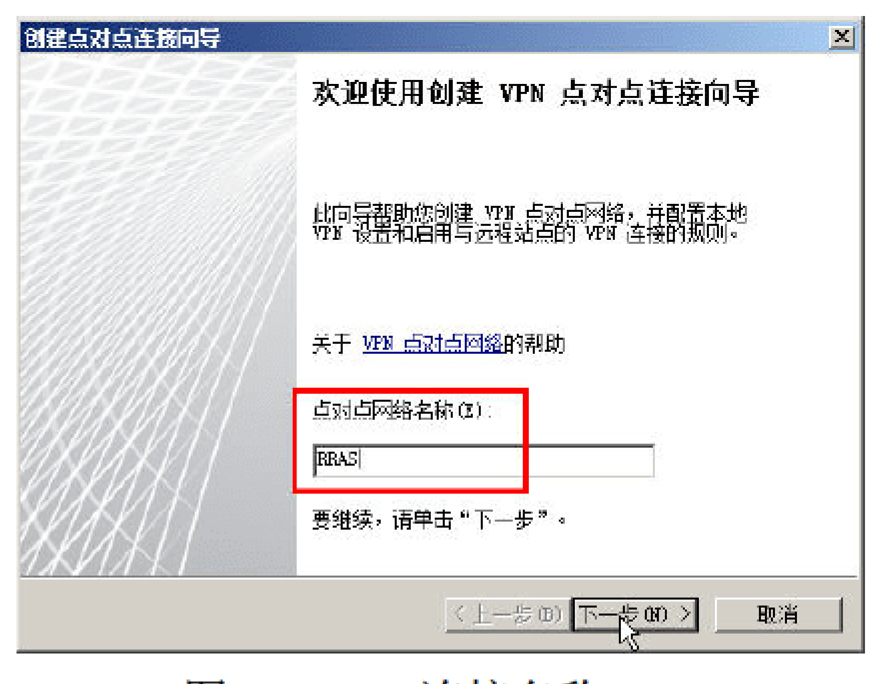


图 16-150 连接名称

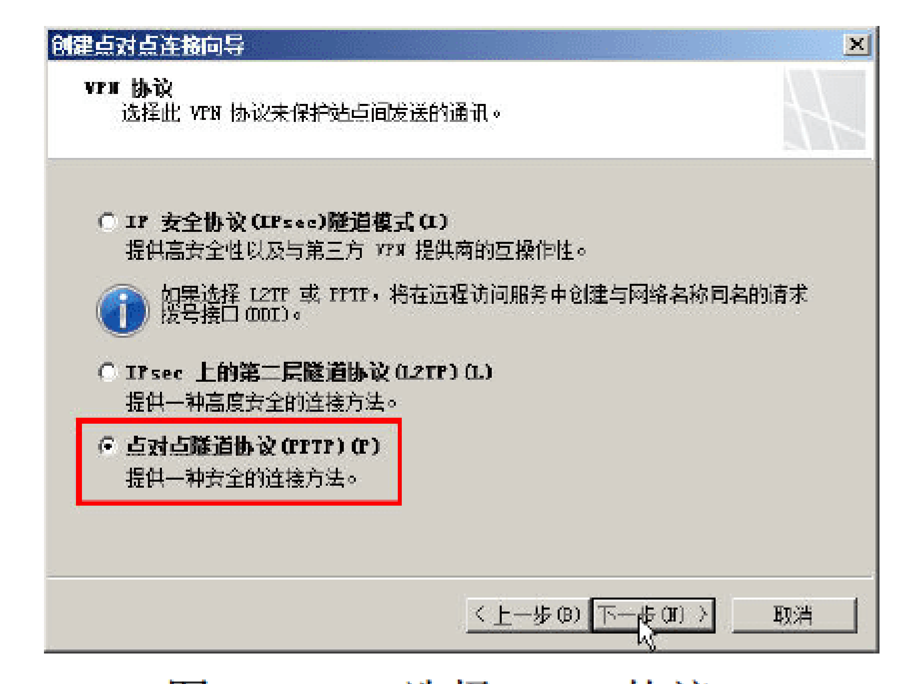
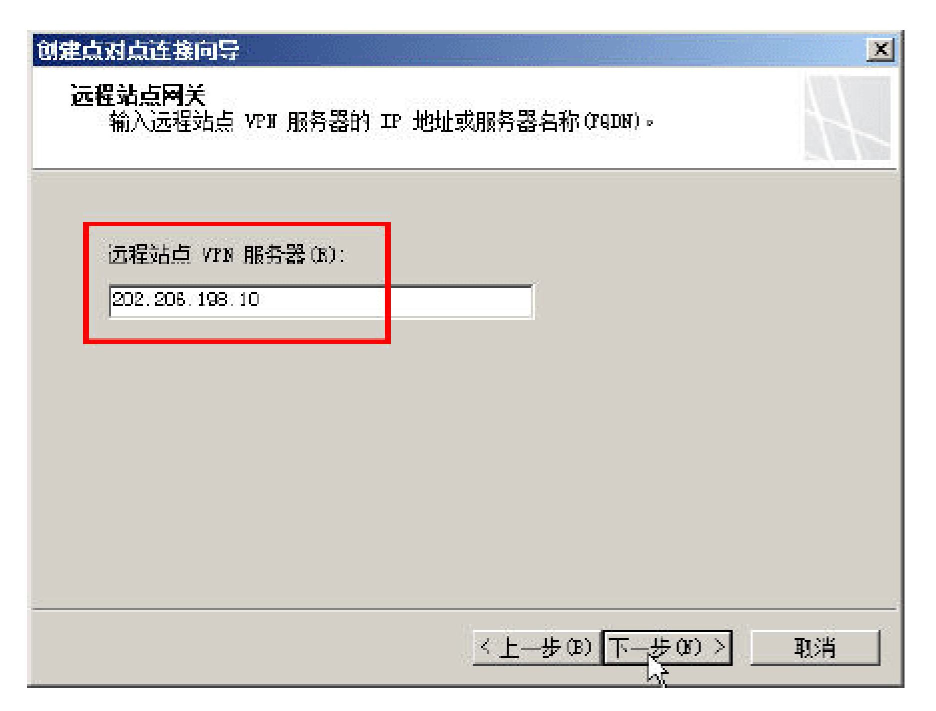
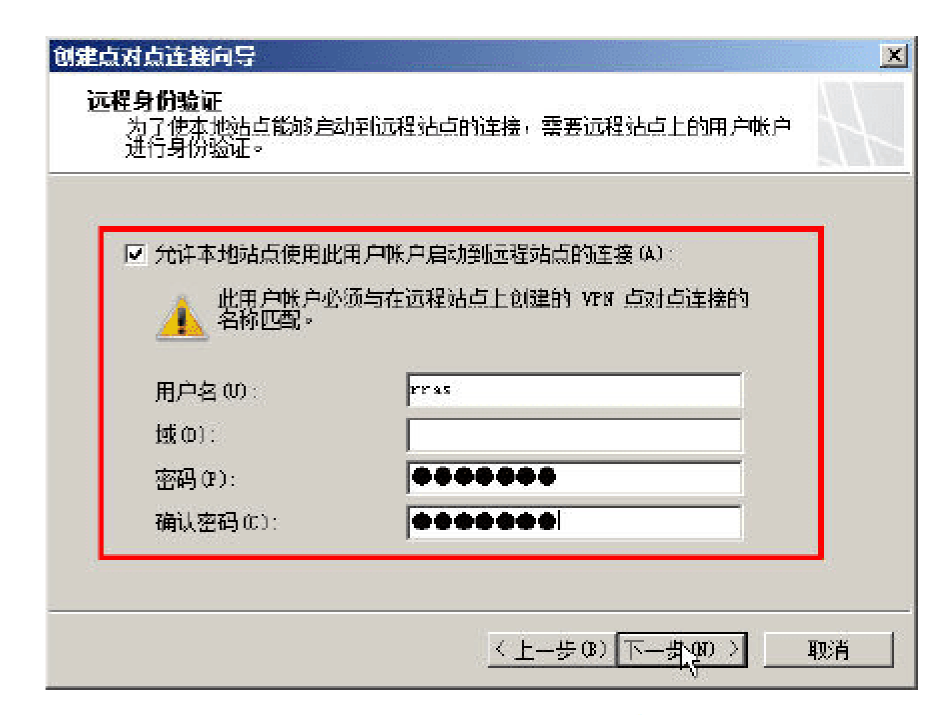


图 16-151 选择 PPTP 协议

04 在“远程站点网关”对话框中，输入网络 2 中 Forefront TMG 的外网 IP，本例为 202.206.198.10，如图 16-152 所示。

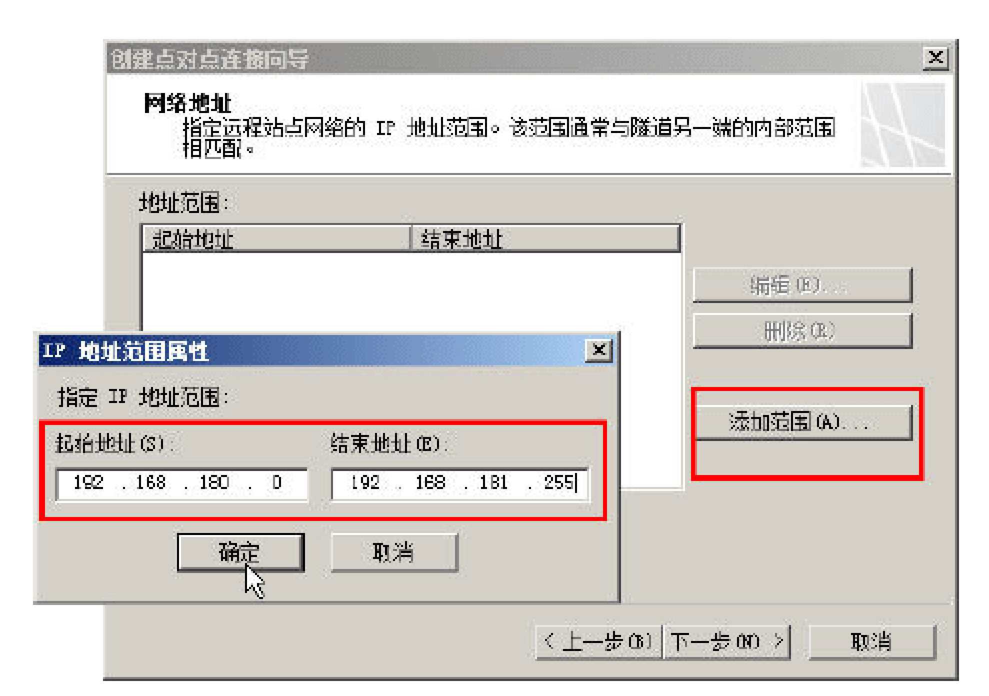
05 在“远程身份验证”对话框中，选中“允许本地站点使用此用户账户启动到远程站点的连接”复选框，在“用户名”对话框中，输入允许远程连接的 VPN 用户。在本例中，设置用户为 rras，并设置密码为 a1b2c3D4（该用户在后面创建），如图 16-153 所示。

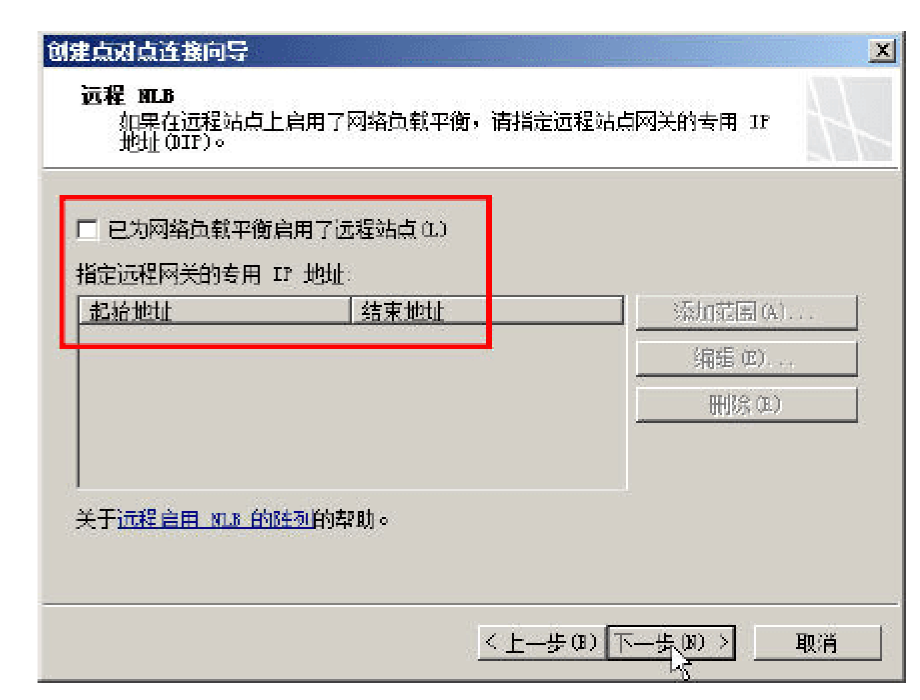

图 16-152　指定远程网关地址


图 16-153　远程身份验证

06 在“网络地址”对话框中，单击“添加范围”按钮，添加网络 2 的“内网”地址。在本例中为 192.168.180.0/24，当然，也可以将网络 2 的 VPN 地址添加进来，如图 16-154 所示。

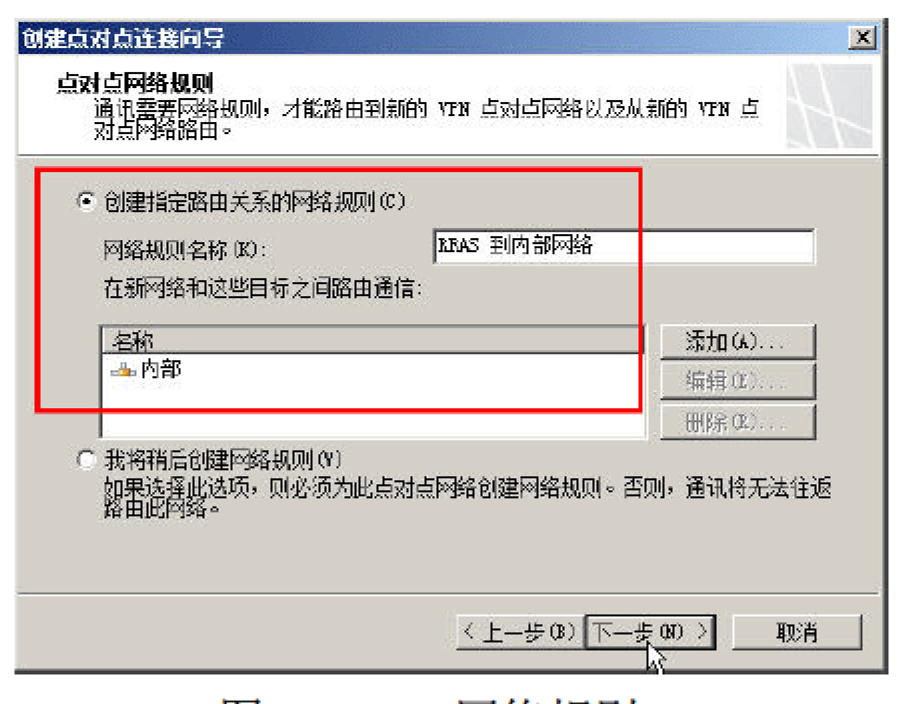
07 在“远程 NLB”对话框中，取消选中“已为网络负载平衡启用了远程站点”复选框，如图 16-155 所示。

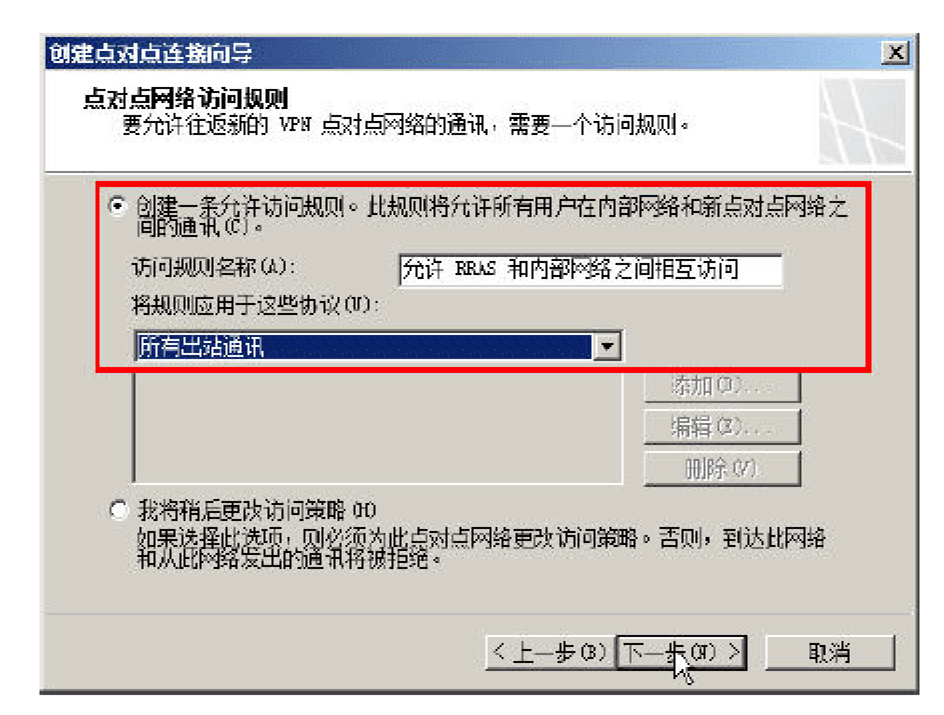

图 16-154　添加远程网络内网地址


图 16-155　远程 NLB

08 在“点对点网络规则”对话框中，选择默认值，将创建网络规则，如图 16-156 所示。

09 在“点对点网络访问规则”对话框中，将创建网络访问规则，并且在“将规则应用于这些协议”下拉列表中，选择“所有出站通讯”选项，如图 16-157 所示。


图 16-156　网络规则


图 16-157　访问规则

10 在“正在完成新建 VPN 点对点网络向导”对话框中，单击“完成”按钮，如图 16-158 所示。

11 在“Forefront TMG”警告对话框中，单击“确定”按钮，如图 16-159 所示。

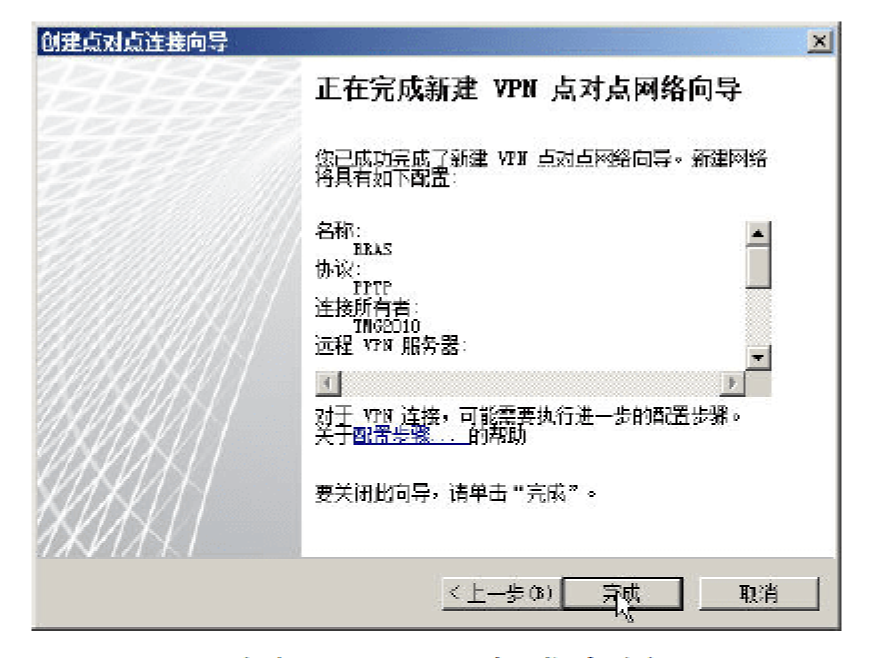




图 16-158　完成向导

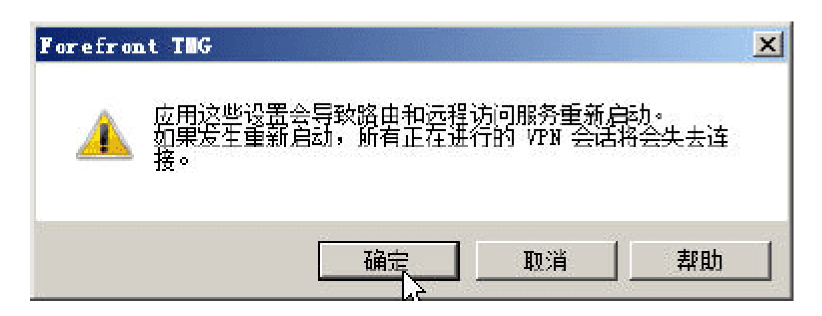


图 16-159　警告

12 在“剩余 VPN 点对点任务”对话框中，单击“确定”按钮，如图 16-160 所示。

13 Forefront TMG 控制台中，单击“应用”按钮，让设置生效，如图 16-161 所示。

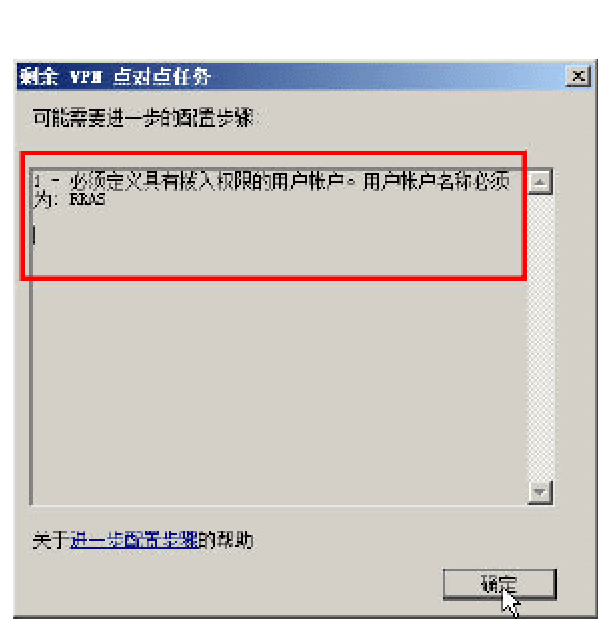


图 16-160　任务

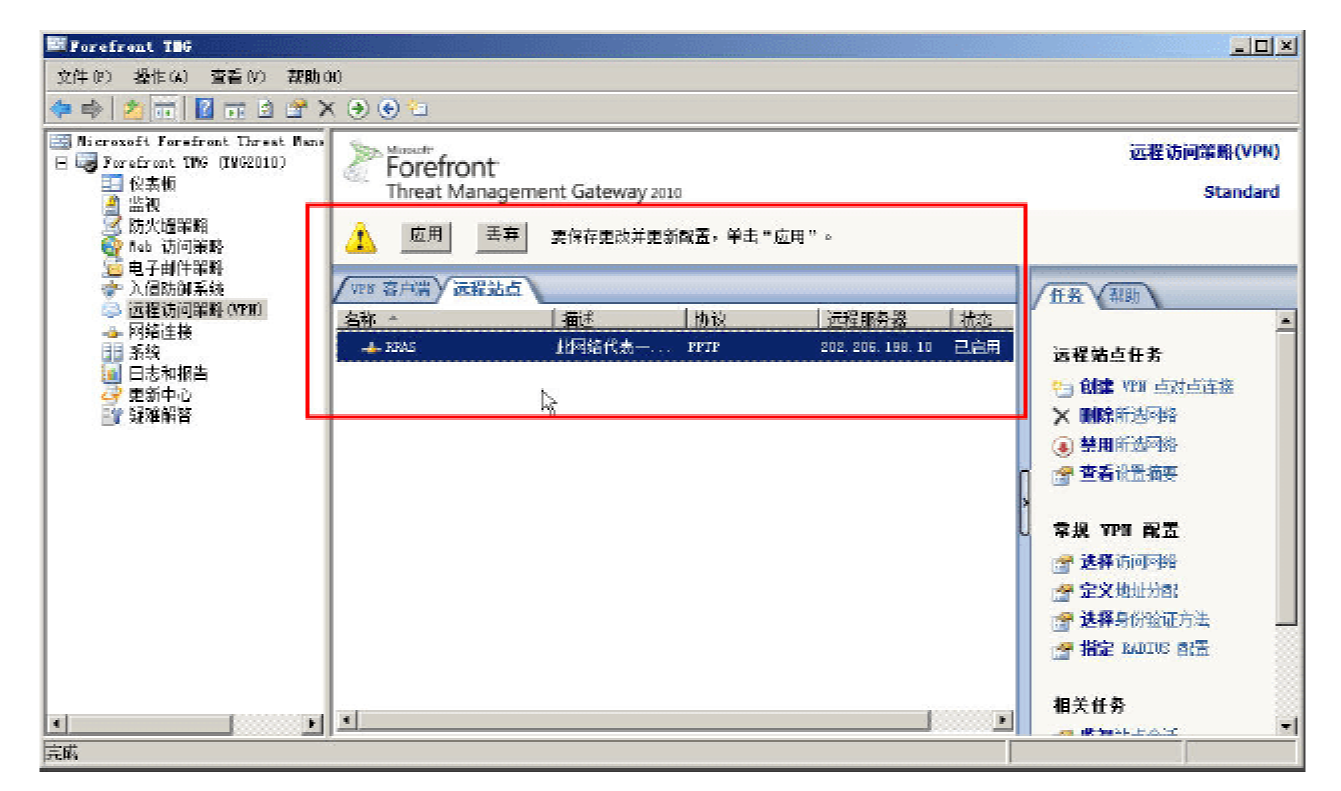


图 16-161　让设置生效

在创建 VPN 站点间路由后，会在“防火墙策略”中添加 1 条策略（图 16-157 中设置），如图 16-162 所示，这是 Forefront TMG 自动创建的，你可以在此查看。

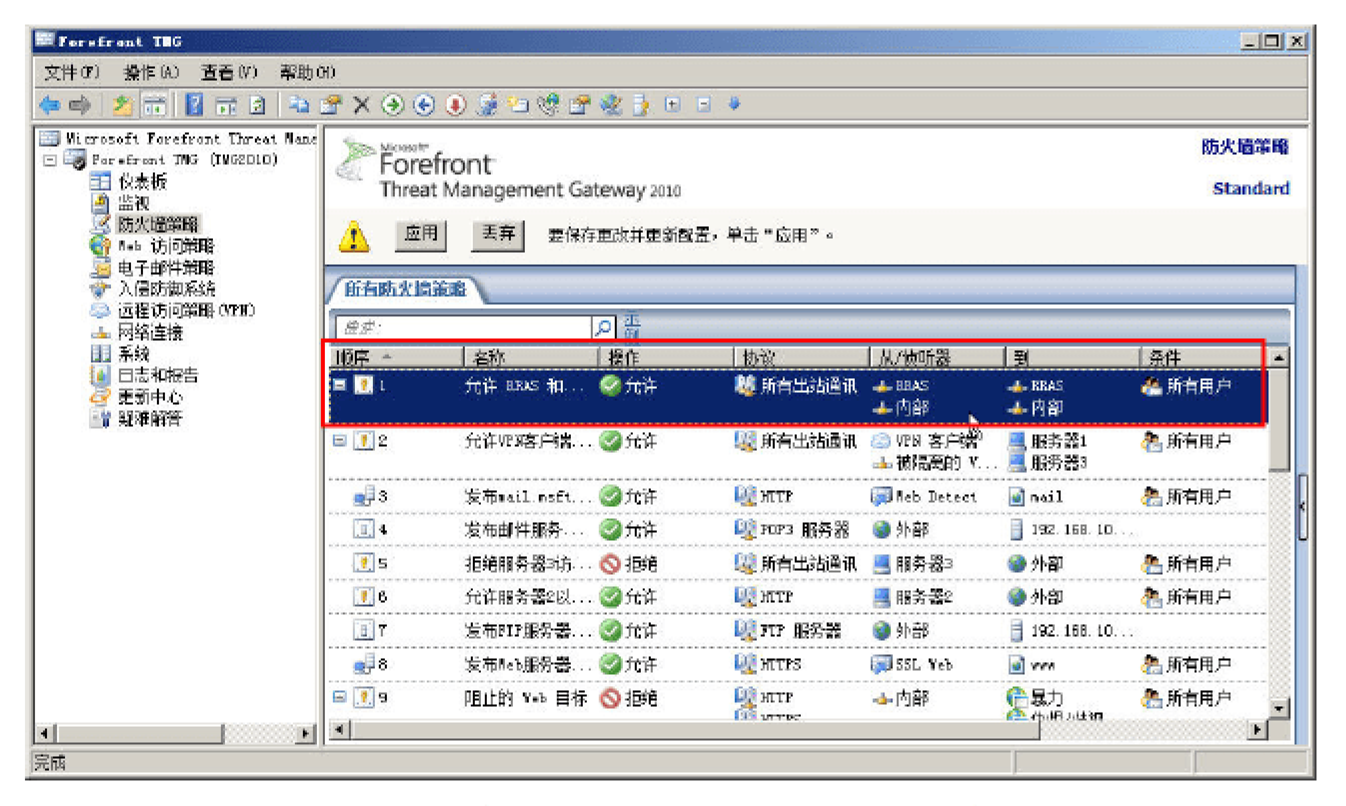


图 16-162　添加 VPN 站点间路由后添加的策略

另外，在“网络连接”中，还会创建名为 RRAS 的连接，并指明其关系，如图 16-163 所示。

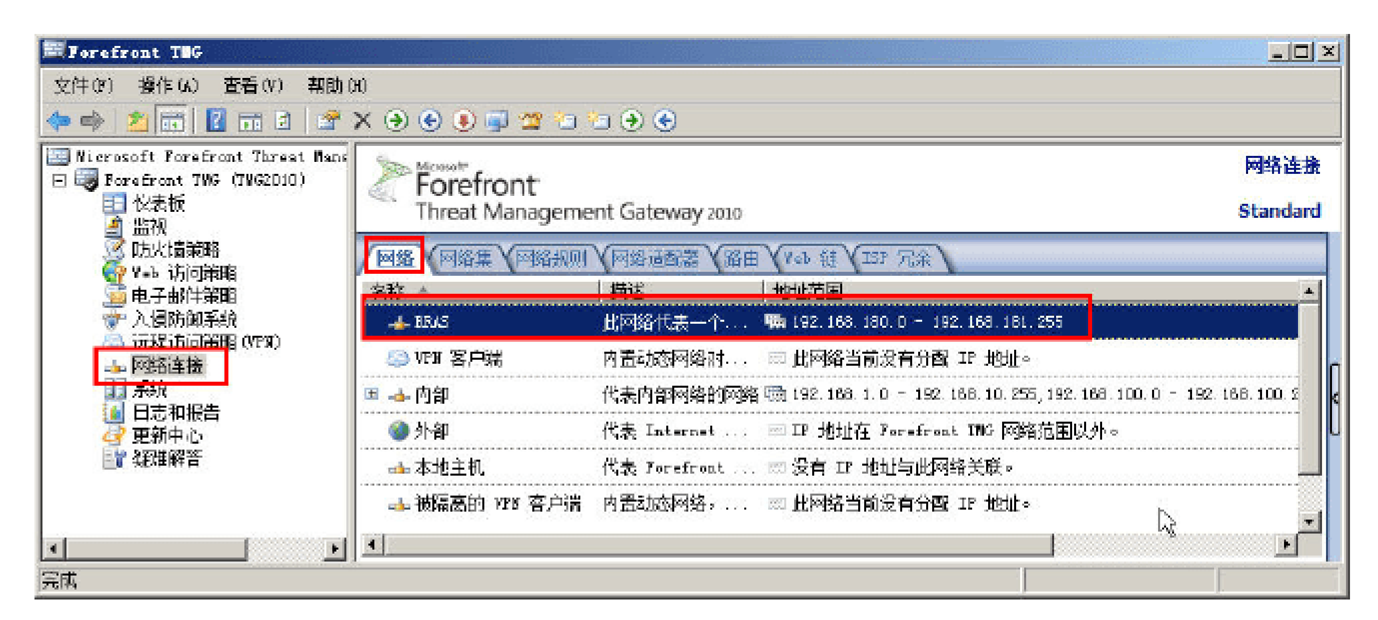


图 16-163　网络连接

然后进入“服务器管理器→配置→本地用户和组→用户”中，添加名为 rras、密码为 a1b2c3D4 的用户（如图 16-164 所示），并且设置“允许拨入”权限，这些不再赘述。

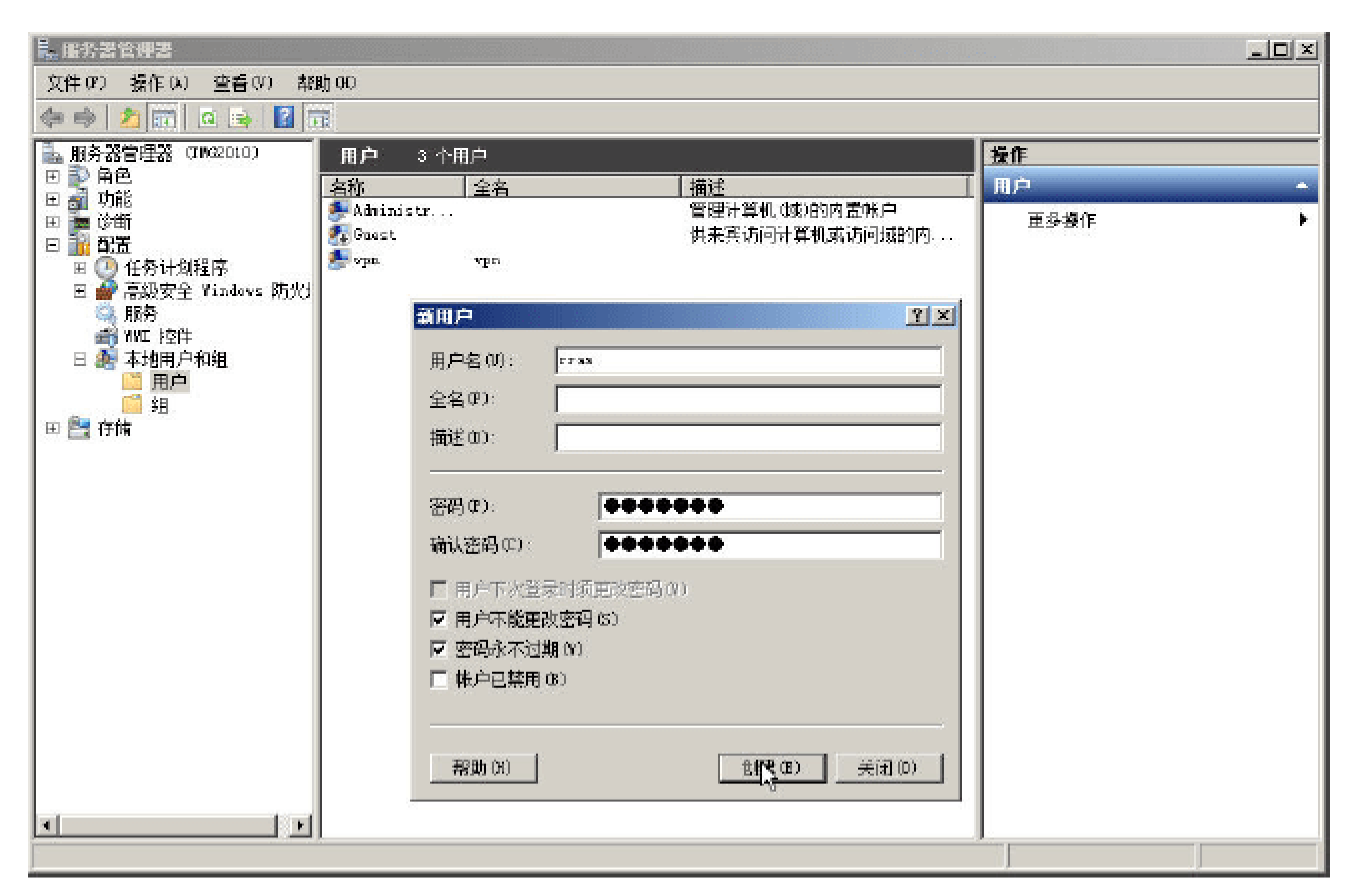


图 16-164　创建用户

在“网络 2”的 Forefront TMG 中，同样也要创建“VPN 点对点连接”，主要步骤与上文相似，但需要注意以下不同之处：

（1）在“远程站点网关”对话框中，指定远程站点 VPN 服务器为“网络 1”的 Forefront TMG 的外网地址，本例中为 202.206.197.125，如图 16-165 所示。

（2）在“网络地址”对话框中，指定“网络 1”的内网地址，本例为 192.168.1.0～192.168.10.255、192.168.100.0～192.168.100.255、192.168.254.0～192.168.254.255，如图 16-166 所示。

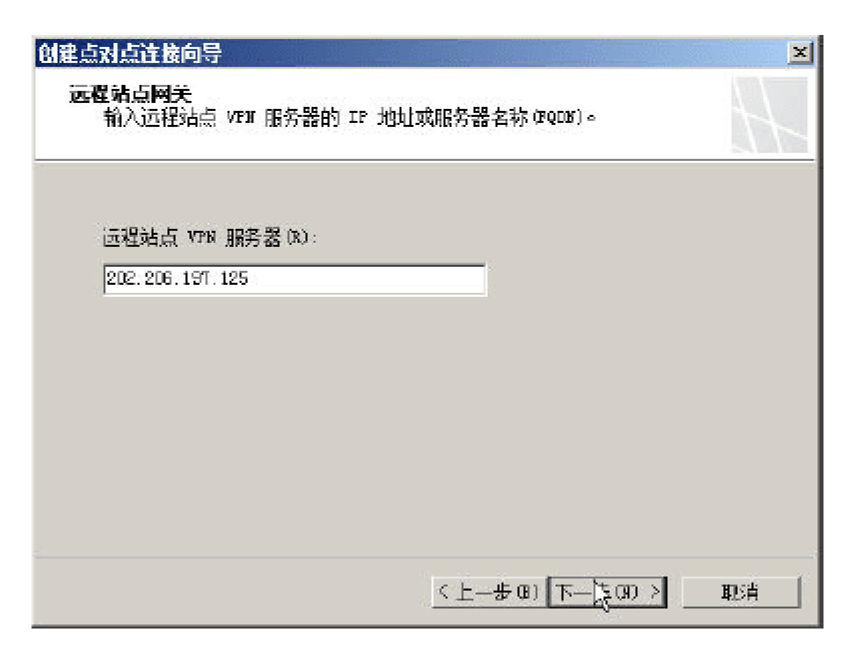


图 16-165　远程站点网关

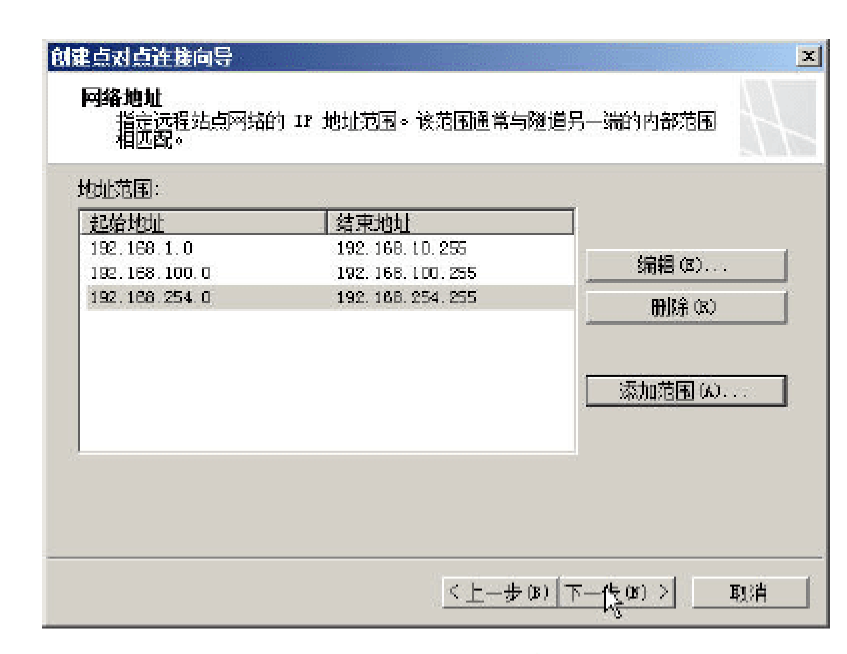


图 16-166　网络 1 内网地址

（3）其他则与上文步骤完全一致。

创建完成之后，在两个网络之间将创建 VPN 路由，并且在由内部网络访问另一网络内部地址的时候，Forefront TMG 自动完成 VPN 站点间路由的连接工作。当然，如果网络中有三层交换机，需要在三层交换机中，将到另一网络的静态路由，指向所属网络的 Forefront TMG 的内网 IP 地址，这样才能正确访问。

16.7　组建基于 SSTP 的 VPN 网络

要组建基于 SSTP 的 VPN 网络，需要为 VPN 服务器申请一个“服务器证书”并保存在“计算机存储”中。一般情况下，可以选择 Windows Server 2003 或 Windows Server 2008 的“证书服务器”。证书服务器分两种：一种是需要 Active Directory 的“企业证书服务器”，另一种是“独立证书服务器”。如果只是需要“服务器证书”。一般选择“独立证书服务器”。当然，选择“企业证书服务器”也是可以的，只是“独立证书服务器”相对比较简单。在本节中，通过图 16-167 所示的网络拓扑进行学习。

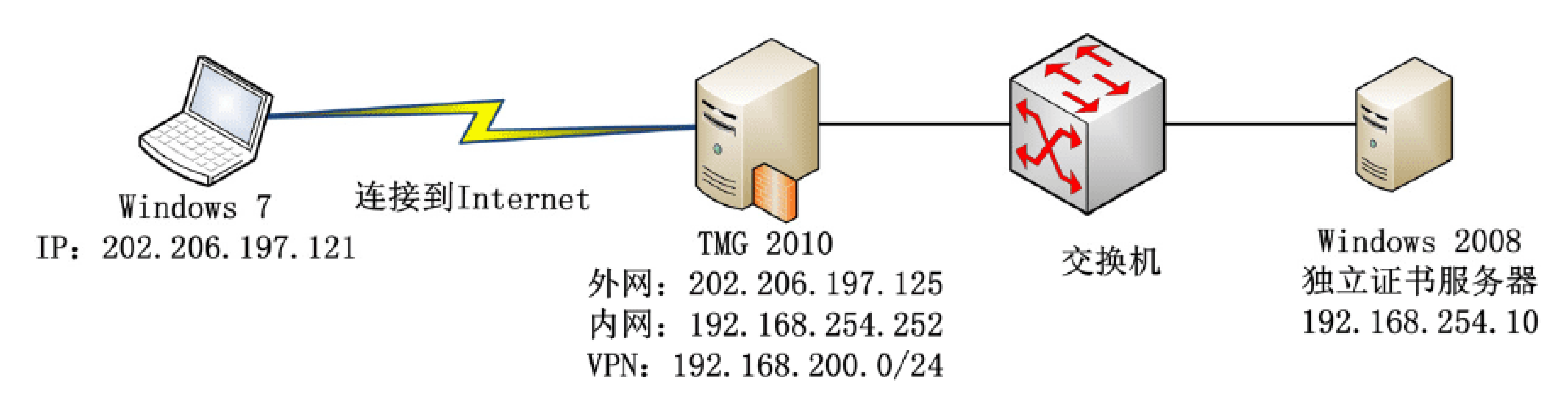


图 16-167　基于 SSTP 协议的 VPN 网络

本次案例要实现的功能：

（1）Forefront TMG 从内部的 Windows Server 2008 申请证书。

（2）Forefront TMG 将 Windows Server 2008 的“证书服务”（Web 服务器）发布到 Internet。

（3）Windows 7 从 Forefront TMG 发布的证书服务器下载“根证书”并保存到“可信任的证书颁发机构”。

（4）Windows 7 使用 SSTP 协议呼叫 Forefront TMG 2010 的 VPN 服务器。呼叫成功后，获得 192.168.200.0～192.168.200.255 之间的地址，并能访问 192.168.254.10。

（5）使用 SSTP 协议时，VPN 服务器需要与一个域名“绑定”。在本例中，该域名为 sstp.msft.com，在 VPN 客户端，需要能将该域名解析为 VPN 服务器的外网 IP 地址。如果不能解析，则需要修改 VPN 客户端的 hosts 文件。

16.7.1　实现步骤

基于 SSTP 协议的 Forefront TMG 的 VPN 网络组建的主要步骤如下。

01 准备独立证书服务器。

02 在 Forefront TMG 计算机上创建策略，从独立证书服务器申请证书并保存在计算机存储中。

03 在 Forefront TMG 上创建“Web 服务器发布策略”，发布证书服务器到 Internet。在本例中，对外发布名为 ca.msft.com。

04 为 Forefront TMG 启用 VPN 网络访问，并使用 SSTP 协议。在本例中，VPN 服务器的对外服务名为 sstp.msft.com。

05 VPN 客户端从证书服务器下载根证书并安装。

06 VPN 客户端使用 SSTP 协议拨号 VPN 服务器。

下文将详细介绍每一个步骤。

16.7.2 安装独立证书服务器

在网络中的一台 Windows Server 2008（或 Windows Server 2008 R2）的计算机上，配置 IP 地址、测试网络连通性、安装独立证书服务器，步骤如下。

01 根据图 16-167 所示的网络拓扑，为 Windows Server 2008 设置 IP 地址 192.168.254.10，设置网关地址为 192.168.254.252，如图 16-168 所示。

02 设置完成后，进入命令提示符，使用 ping 命令，测试到 Forefront TMG 的连通性，如图 16-169 所示。只有在网络连通后，才能继续后面的操作。

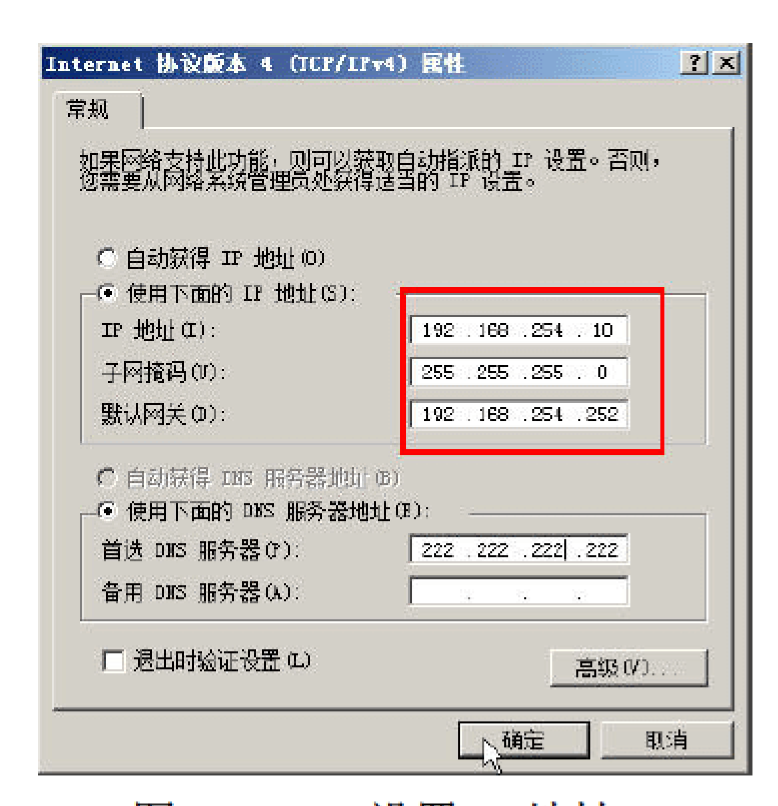


图 16-168 设置 IP 地址

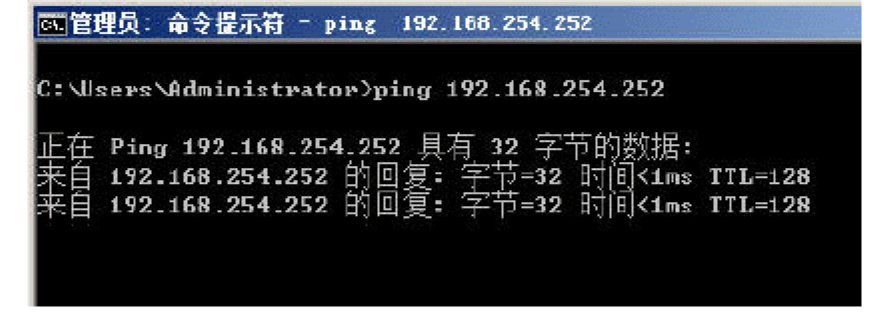


图 16-169 测试网络连通性

如果不能 ping 通，则需要在 Forefront TMG 上添加“访问规则”，允许 ping 通（访问规则的创建可参见后文）。

当网络正常之后，安装标准证书服务器，步骤如下。

01 进入“服务器管理器”，单击“添加角色”链接，如图 16-170 所示。

02 在“选择服务器角色”对话框中，选中“Active Directory 证书服务”复选框，如图 16-171 所示。

03 在“选择角色服务”对话框中，在“角色服务”选项组中，选中“证书颁发机构”与“证书颁发机构 Web 注册”复选框，在弹出的“添加角色向导”对话框中，单击“添加必需的角色服务”按钮，如图 16-172 所示。

04 在“指定安装类型”对话框中，选中“独立”单选按钮，如图 16-173 所示。

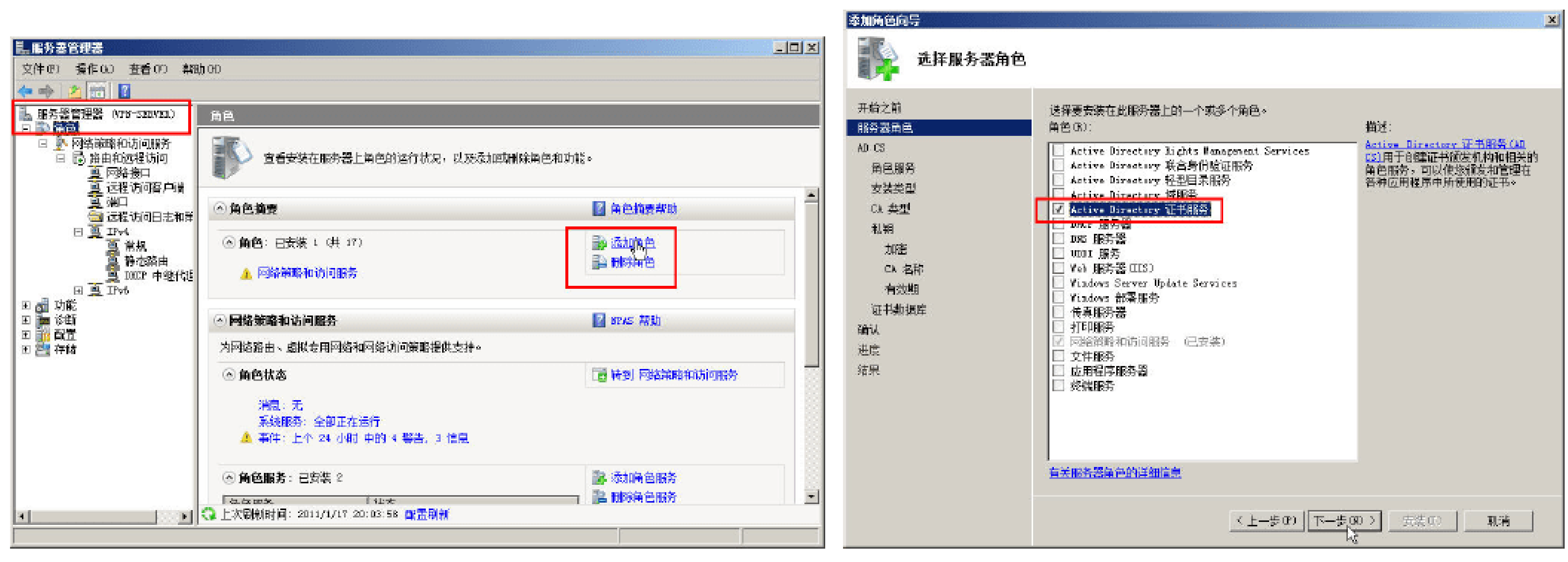


图 16-170　添加角色　　　　图 16-171　添加证书

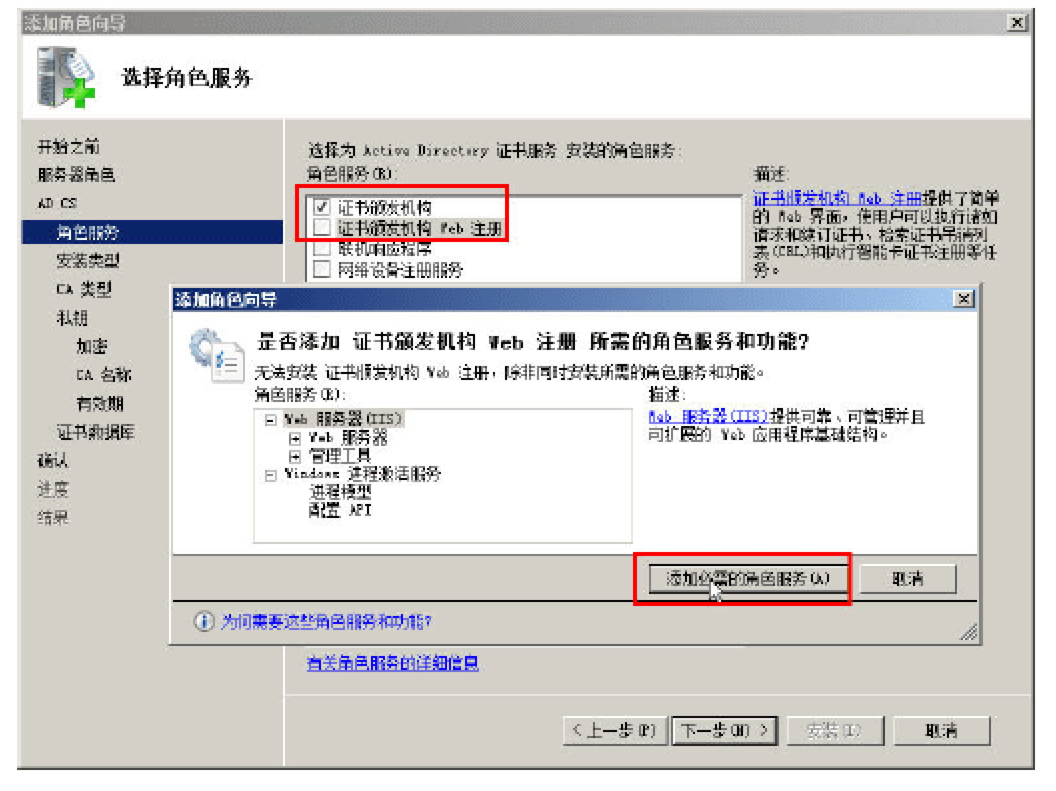
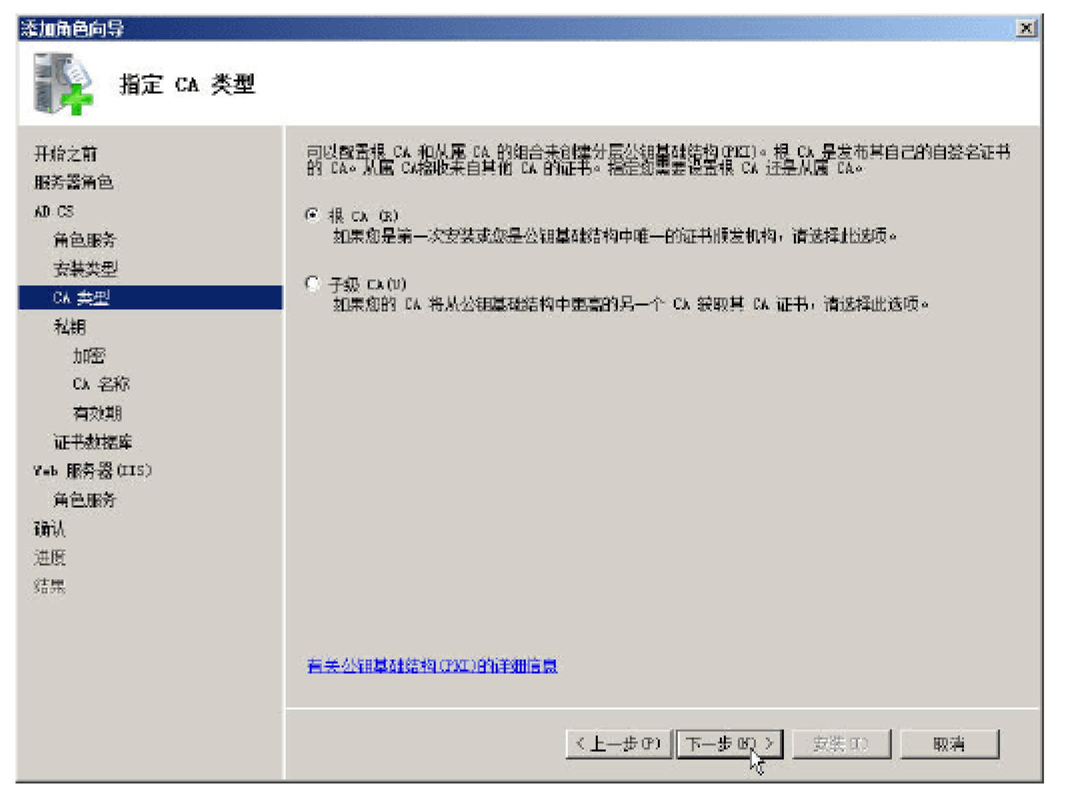


图 16-172　添加证书颁发机构　　　　图 16-173　安装独立证书

05 在“指定 CA 类型”对话框中，选中“根 CA”单选按钮，如图 16-174 所示。

06 在“设置私钥”对话框中，选中“新建私钥”单选按钮，如图 16-175 所示。



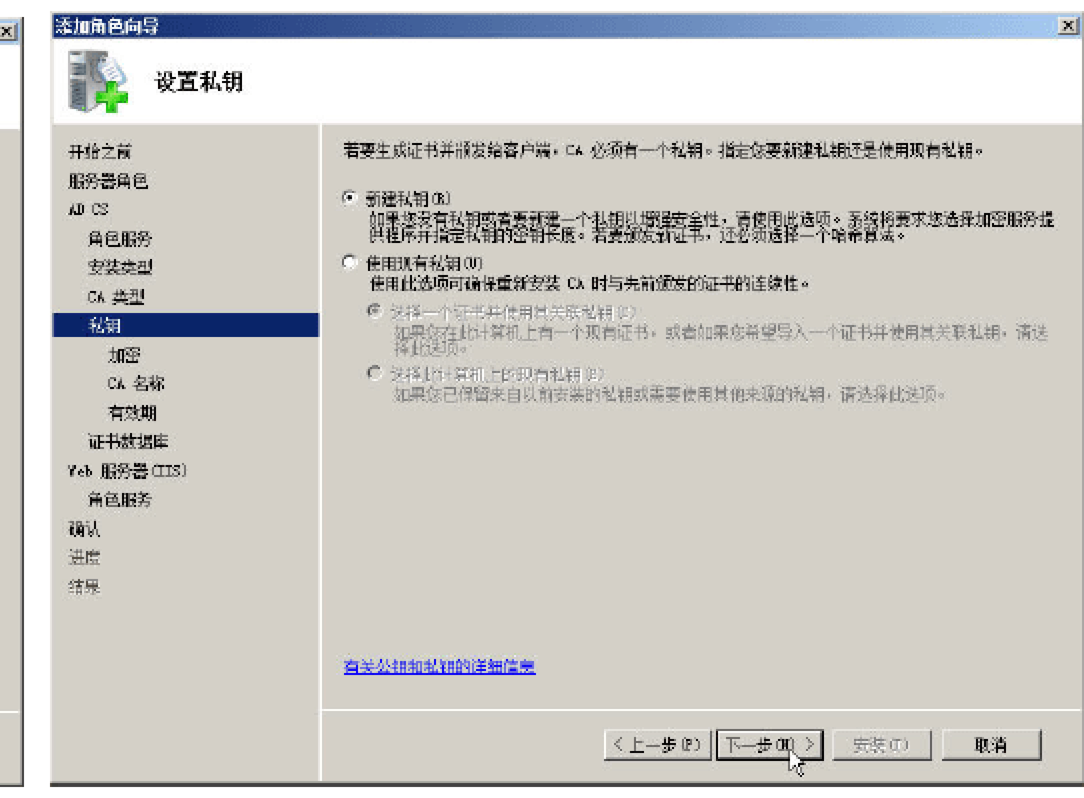


图 16-174　创建根 CA　　　　图 16-175　新建私钥

07 在“为 CA 配置加密”对话框中，选择默认值，如图 16-176 所示。

08 在“配置 CA 名称”对话框中 ，设置 CA 的名称。在实验中，可以选择默认值（是计算机名称加“短横线”加“CA”），如图 16-177 所示。

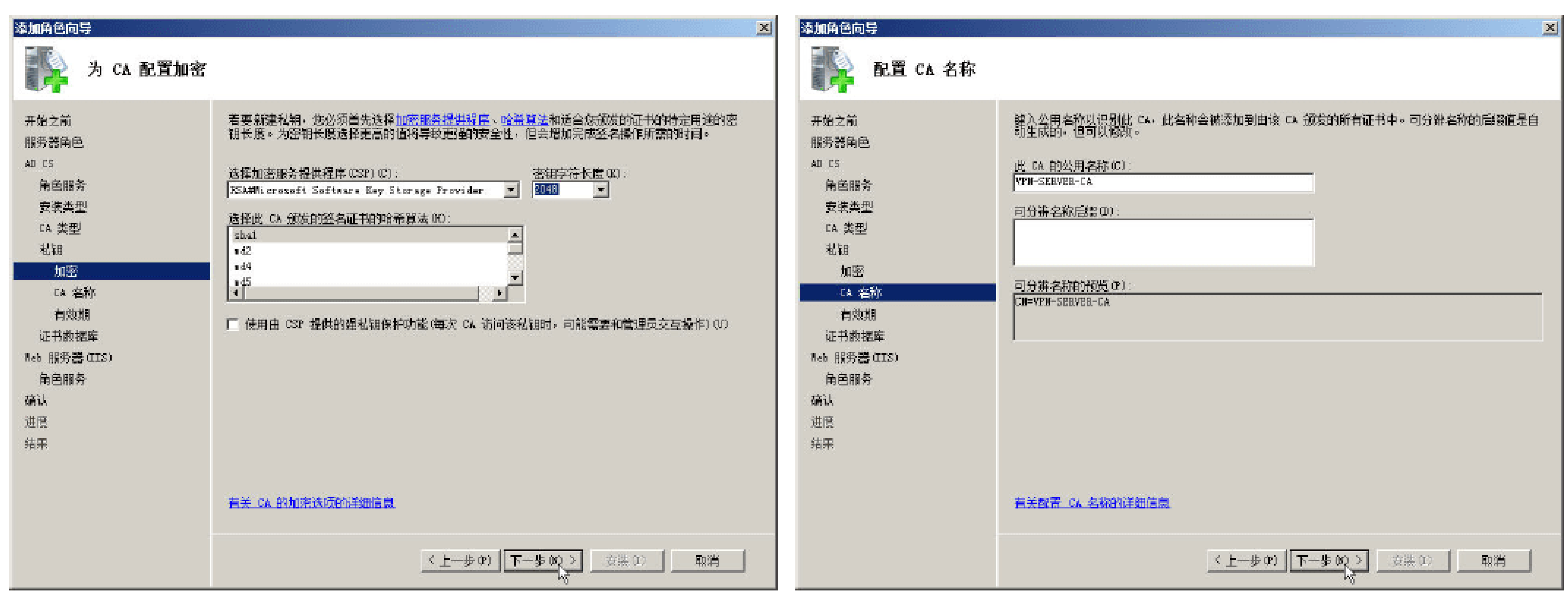


图 16-176 为 CA 配置加密　　　图 16-177 设置 CA 的公用名称

09 在“设置有效期”对话框中，选择此 CA 生成的证书的有效期，如图 16-178 所示。在 Windows Server 2008 中，标准证书服务器的有效期是 5 年。如果组建商用的 VPN 服务器，可以根据需要，设置证书服务器的有效时间。当然，商用 VPN 服务器即使证书服务器过期，也可以重新安装、重新为服务器申请证书，这个并不影响实际的商业使用。

10 在“配置证书数据库”对话框中，选择证书数据库与证书日志的保存位置，在此选择默认值即可，如图 16-179 所示。



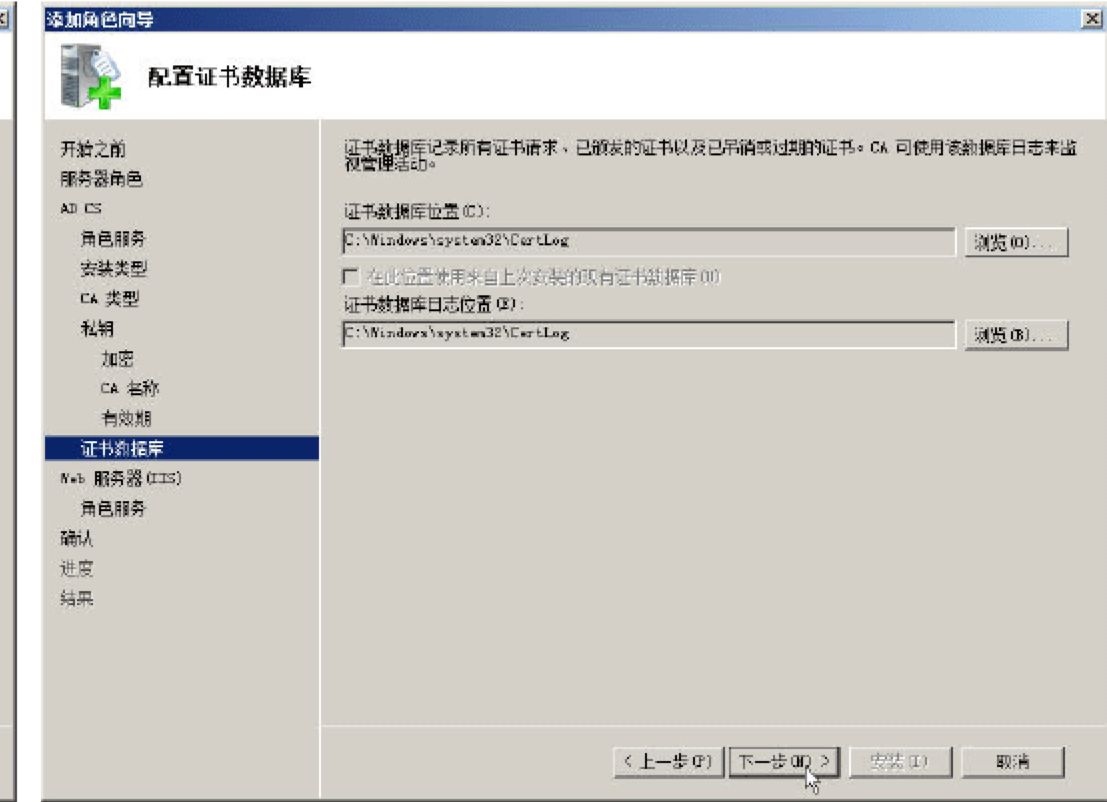


图 16-178 设置有效期　　　图 16-179 证书数据库保存位置

11 在“Web 服务器”对话框中，显示了 Web 服务器（IIS）的简要信息，如图 16-180 所示。

12 在随后出现的“选择角色服务”对话框中，显示并默认选中了安装“证书颁发机构 Web 注册”所需要的 Web 服务器组件，在此保持默认值即可，如图 16-181 所示。

13 在“确认安装选择”对话框中，显示了将要安装的独立证书服务器的相关消息，确认无误之后，单击“安装”按钮，如图 16-182 所示。

14 随后 Windows Server 2008 安装程序，将开始独立证书服务器的安装，直到安装完成，如图 16-183 所示。

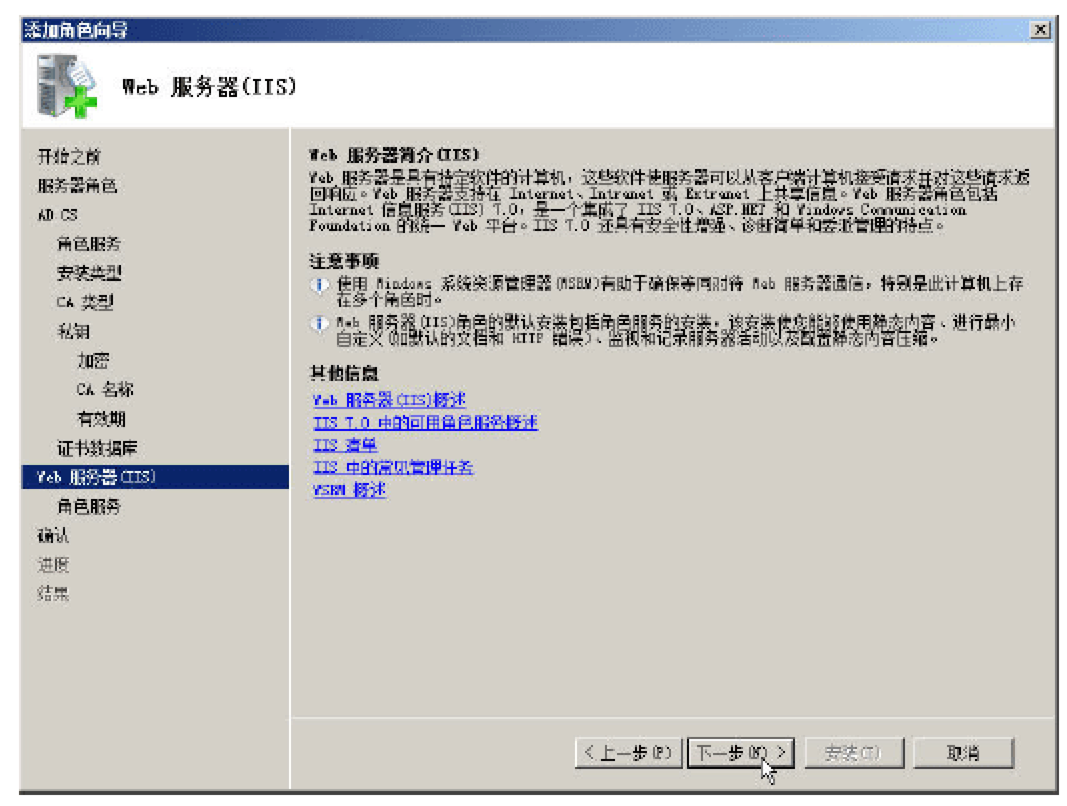


图 16-180　Web 服务简介

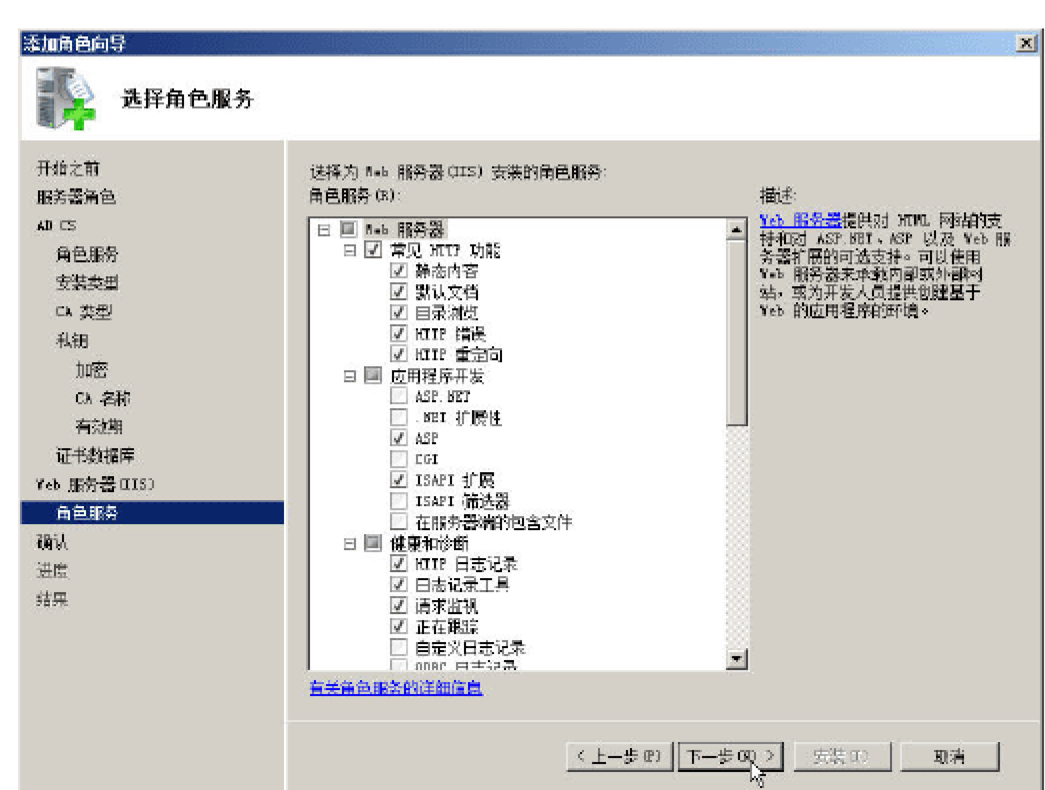


图 16-181　证书注册所需要的 Web 服务



图 16-182　安装前确认信息

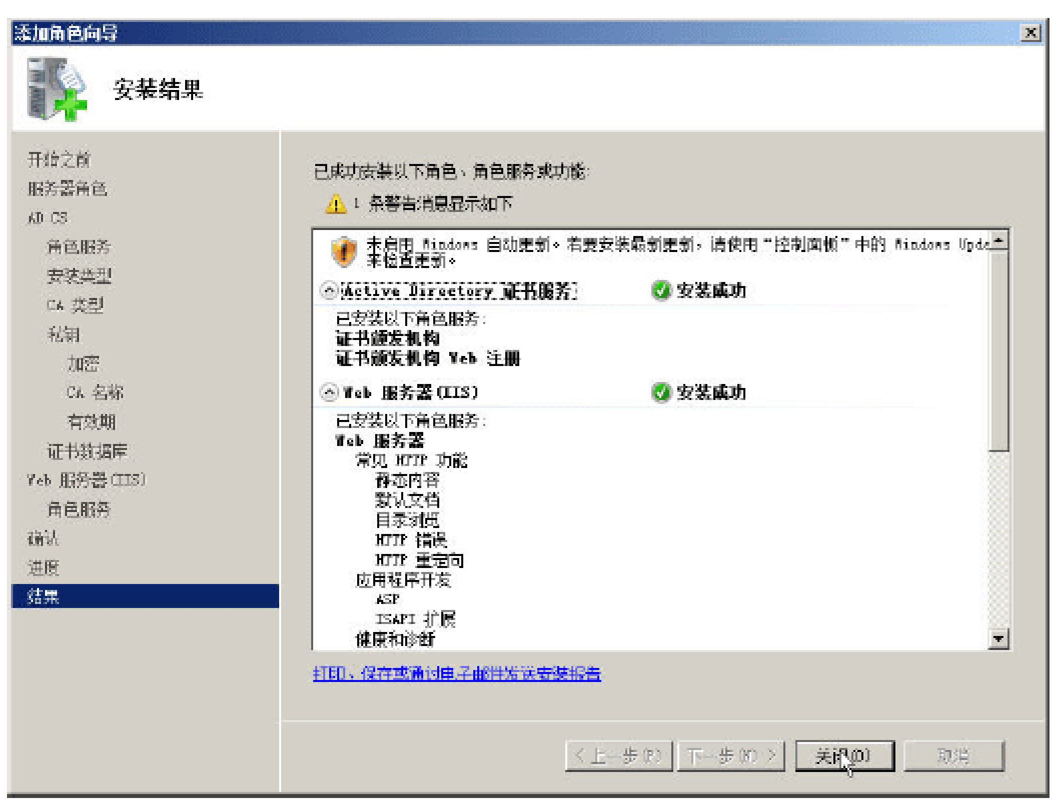


图 16-183　安装完成

16.7.3　配置证书服务器

在安装完标准证书服务器后，为了简化实验的步骤，可以将标准证书服务器配置成“自动颁发申请的证书”；另外，为了让客户端计算机（包括 Forefront TMG），验证证书服务器的吊销列表，需要单独修改 CRL（如果证书服务器是 Windows Server 2003，则不需要做此设置），其步骤如下。

01 进入“服务器管理器”，定位到“角色→Active Directory 证书服务→STD-CA”，单击鼠标右键，从弹出的快捷菜单中选择“属性”命令，如图 16-184 所示。



说 明

“STD-CA”是证书服务器的计算机名称。

02 在“STDCA-CA 属性”对话框的“扩展”选项卡中，在“选择扩展”下拉列表中选择“CRL 分发点(CDP)”选项，选中“http://ServerDNSName>/CertEnroll/<CaName><CRLNAMESuffix><DeltaCRLAllowed>.crl”一行，然后单击选中“包括在 CRL 中。客户端用它来寻找增量 CRL 的位置。”、“包含在颁发的证书的 CDP 扩展中”、“包括在已发布的 CRL 的 IDP 扩展中”复选框，如图 16-185 所示。

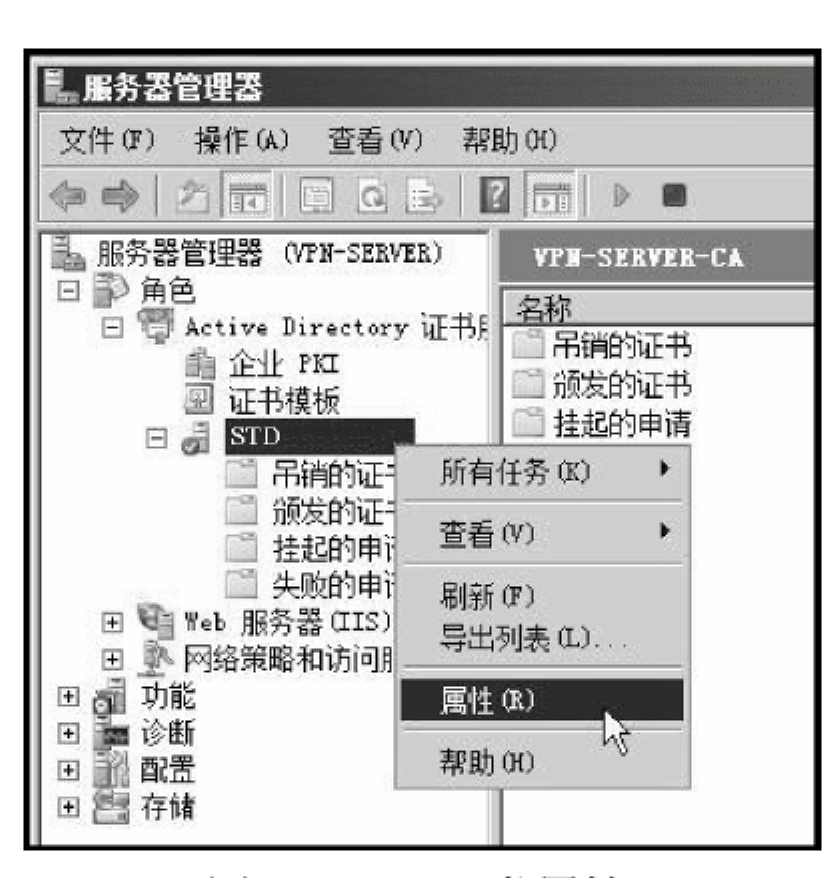



图 16-184　证书属性

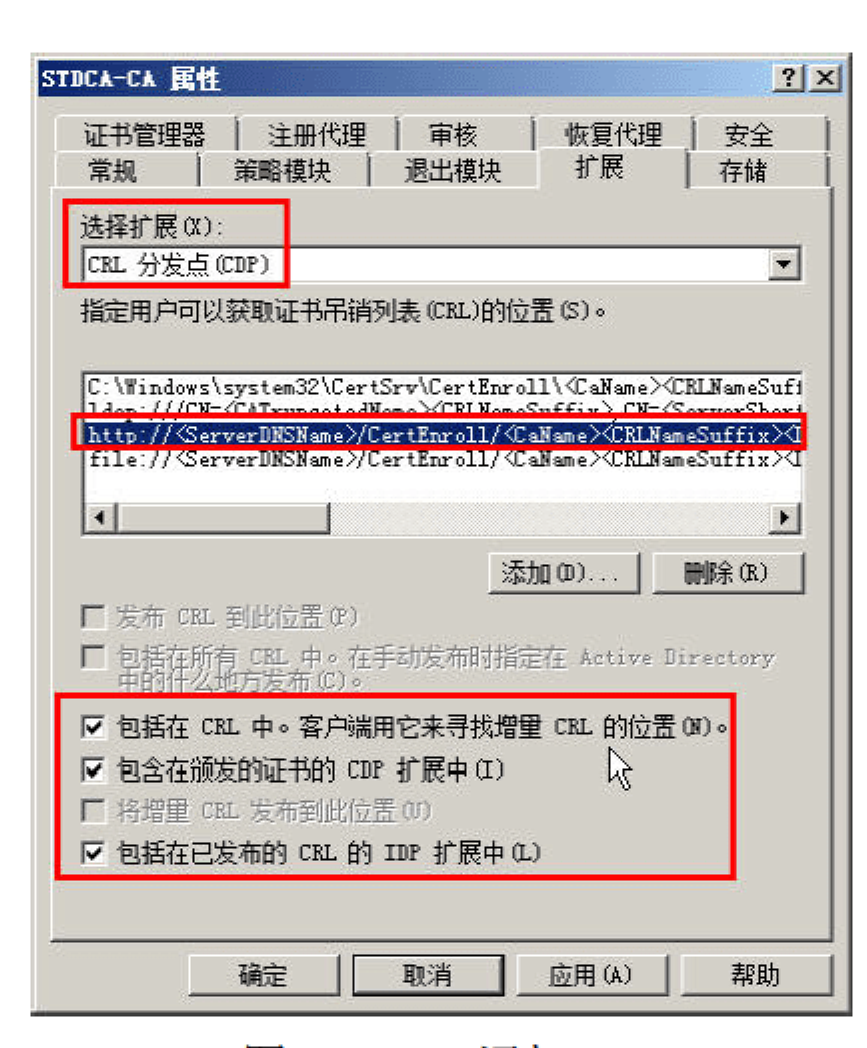


图 16-185　添加 CDP

然后单击“添加”按钮，添加“证书吊销列表”，在添加的时候，添加的站点是 Forefront TMG 发布到 Internet 的对外名称，在本例中是 ca.msft.com，然后再添加证书吊销列表文件所在的虚拟目录及证书吊销列表文件。可以打开“Internet 信息服务管理器”，在默认网站中找到，其虚拟目录为“CertEnroll”，证书吊销列表文件是证书的名称（单击“内容视图”可以看到网站文件）。在本例中，添加的内容为 http://ca.msft.com/certenroll/stdca-ca.crl。为了添加的时候不至于出错，可以通过排列窗口到图 16-186 的方式进行添加，这样填写的时候就比较容易了。

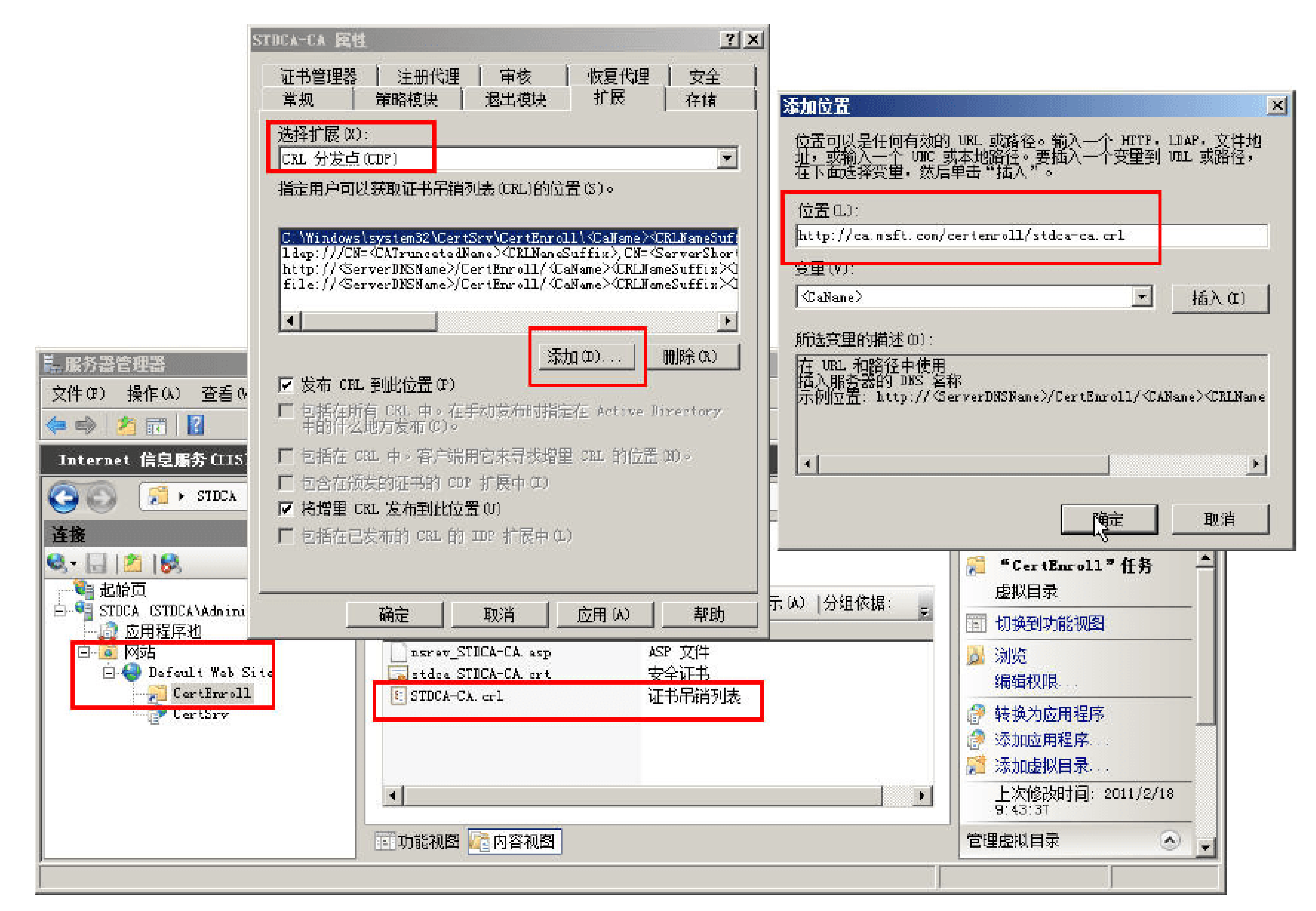


图 16-186　添加 CRL 分发点

添加完成之后，选中“包括在 CRL 中”、“包含在颁发的证书的 CDP 扩展中”、“包括在已发布的 CRL 的 IDP 扩展中”复选框。

03 在“选择扩展”下拉列表中选择“颁发机构信息访问（AIA）”选项，选中“http://ServerDNSName>/CertEnroll/<ServerDNSName><CaName><CertificateName>.crt”一行，然后单击选中“包含在颁发的证书的 AIA 扩展中”、“包括在联机证书状态协议（OCSP）扩展中”复选框，如图 16-187 所示。

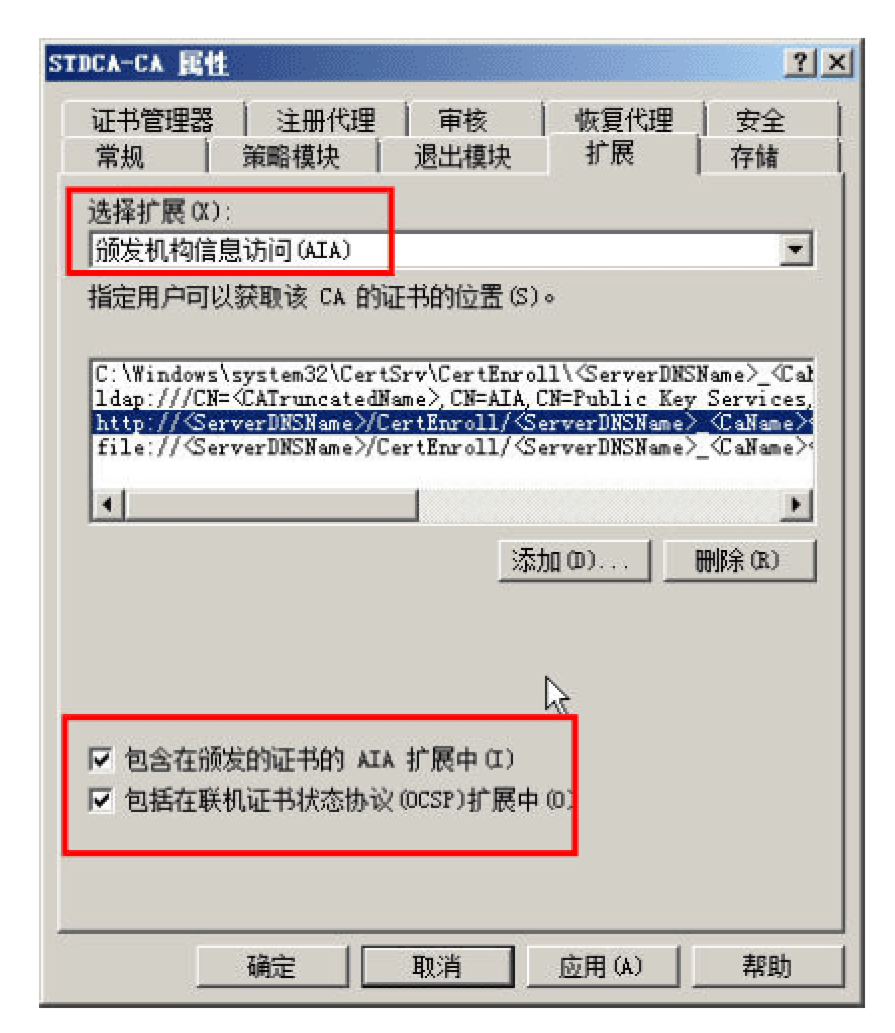


图 16-187　颁发 AIA

然后单击“添加”按钮，添加 http://ca.msft.com/certenroll/stdca-ca.crl，如图 16-188 所示，添加之后，选中“包含在颁发的证书的 AIA 扩展中”、“包括在联机证书状态协议（OCSP）扩展中”。

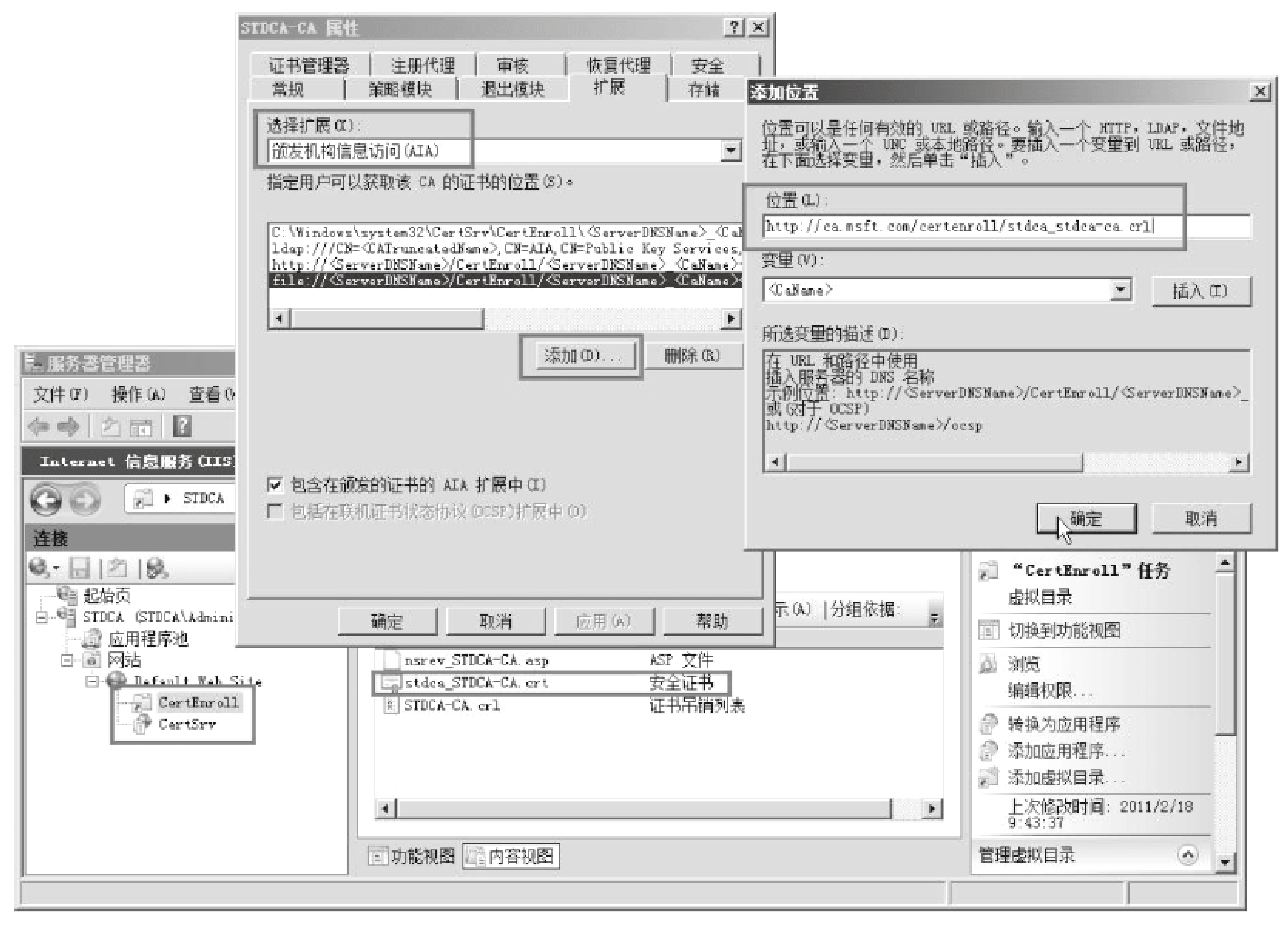


图 16-188　添加 AIA

04 在“策略模块”选项卡中，单击“属性”按钮，在弹出的“属性”对话框中，选中“如果可以的话，按照证书模板中的设置。否则，将自动颁发证书”单选按钮，这样，用户申请的证书

将会自动颁发，如图 16-189 所示。设置完成之后，单击“确定”按钮。

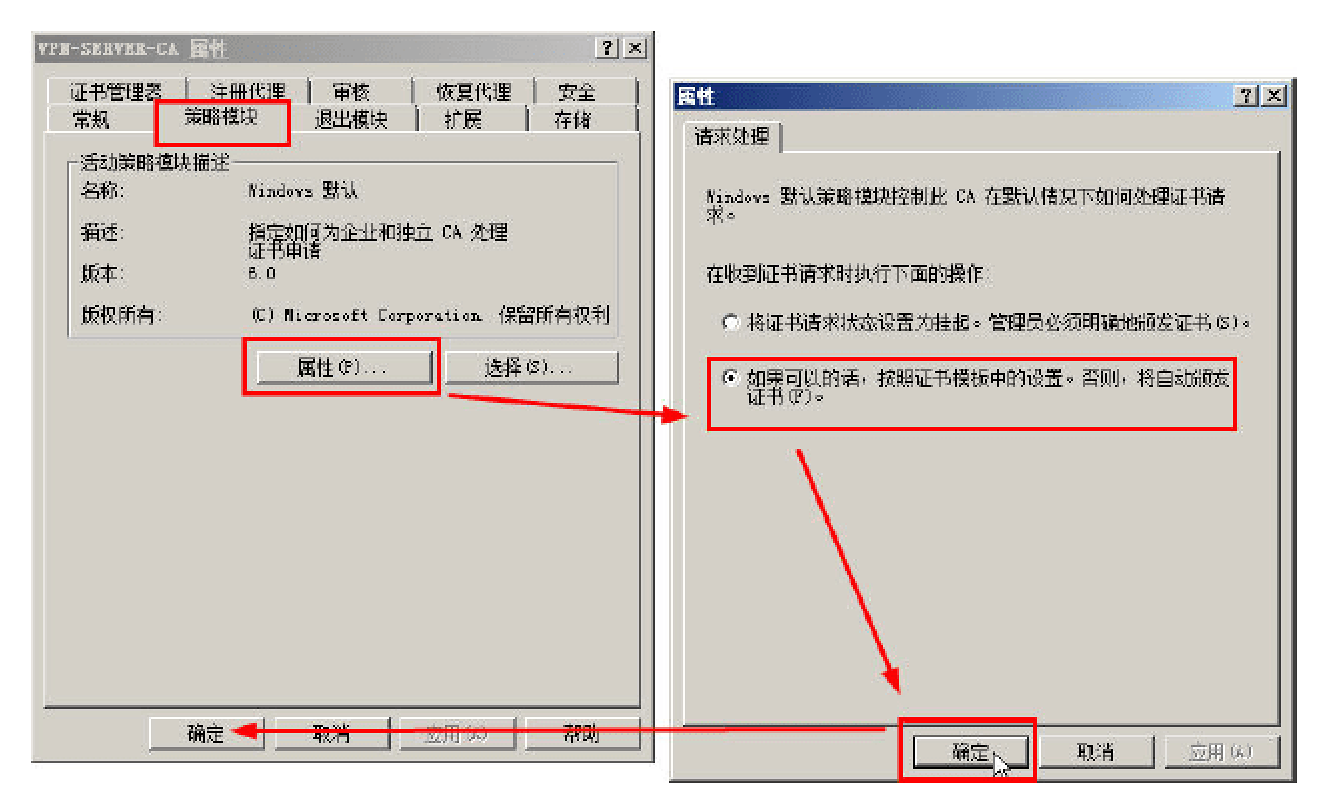


图 16-189　自动颁发证书



说 明

在实验或学习中，为了简化操作步骤，让大家尽快入门，才设置自动颁发证书。在商业使用中，或者在安全性要求较高的地方，最好是保持默认值：让管理员手动颁发每一个申请的证书。

05 配置了证书后，需要让证书服务重新启动才能生效，如图 16-190 所示。

16.7.4　创建访问规则

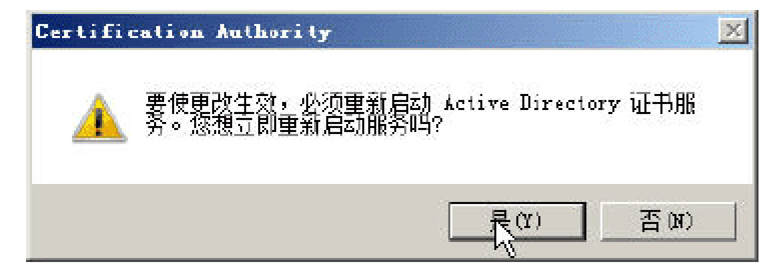


图 16-190　重启让证书服务生效

在 Forefront TMG 的计算机上，创建 2 条访问规则：允许从“任何地点”以“ping”协议访问“任何地址”；另 1 条是允许“本地主机”访问“内部”.其中第 2 条规则，可以参考前文“16.4.2 通过案例介绍访问规则与服务器发布规则”中“1.访问规则 1 的创建”的内容，将“VLAN18”换成“内部”即可。在此主要介绍第 1 条规则的创建，步骤如下。

01 在 Forefront TMG 的控制管理台中，在左侧窗格中右击“防火墙策略”节点，在弹出的快捷菜单中选择“新建→访问规则”命令，如图 16-191 所示。

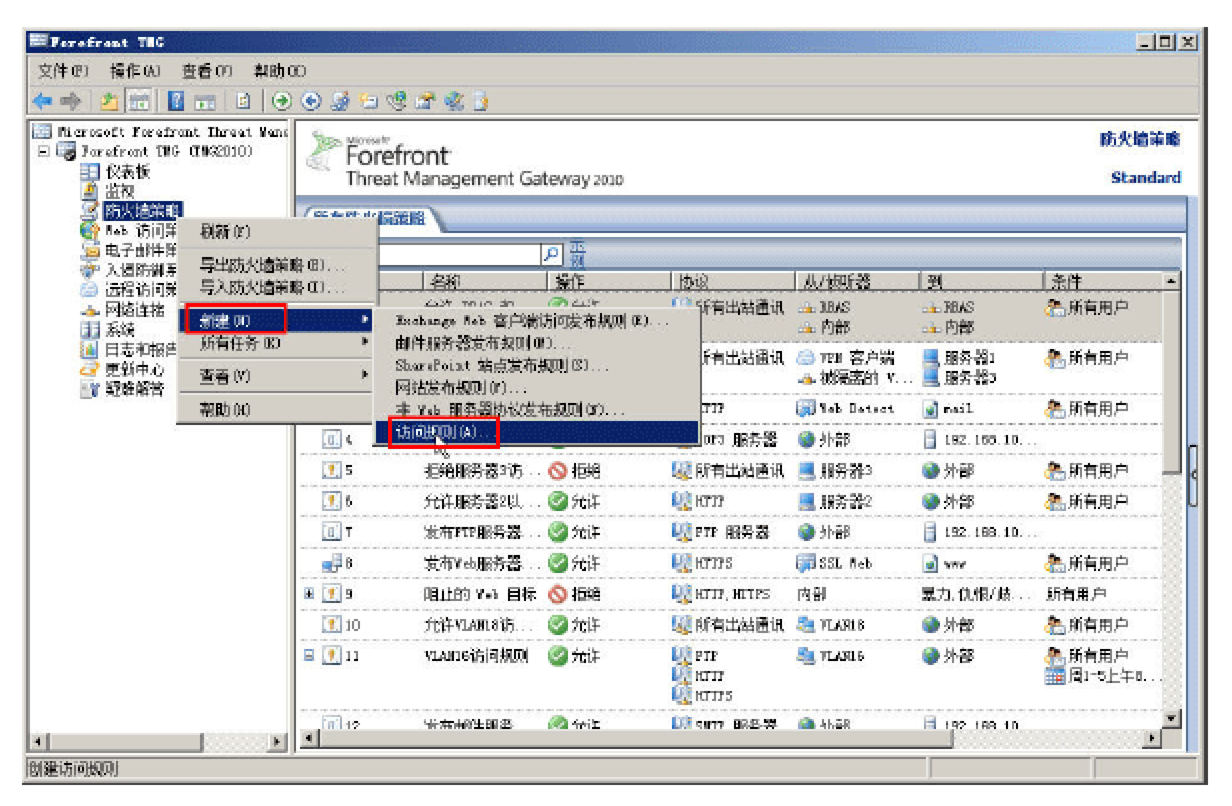


图 16-191

02 在“欢迎使用新建方访问规则向导”对话框中，设置访问规则名称为“ping”，如图 16-192 所示。

03 在“规则操作”对话框中选择“允许”。

04 在“协议”对话框中选择“ping”，如图 16-193 所示。

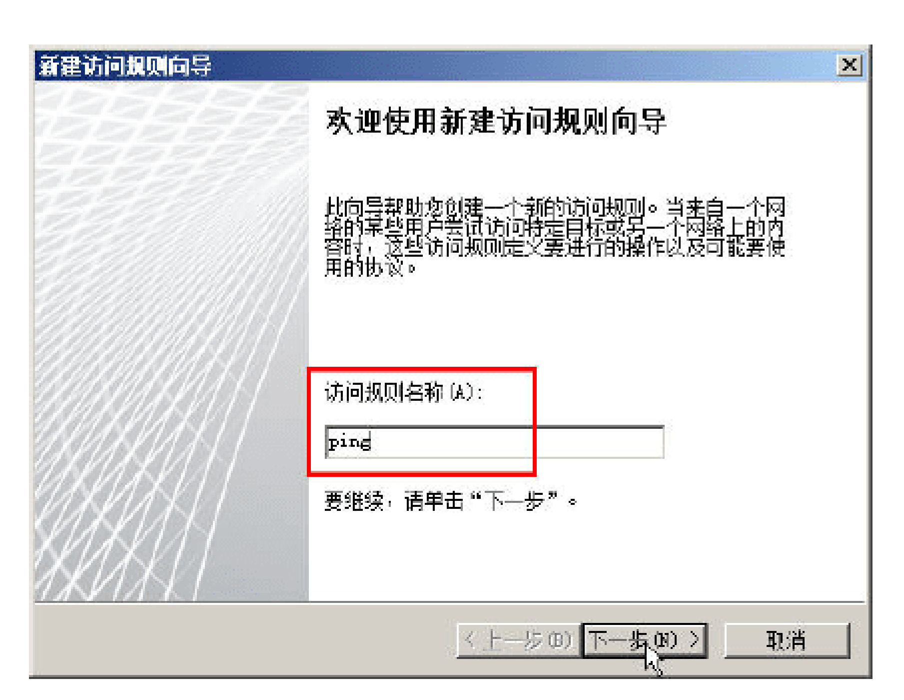


图 16-192 规则名称

图 16-193 选择 ping 协议

05 在“访问规则源”对话框中添加“任何地点”，如图 16-194 所示。

06 在“访问规则目标”对话框中添加“任何地点”，如图 16-195 所示。

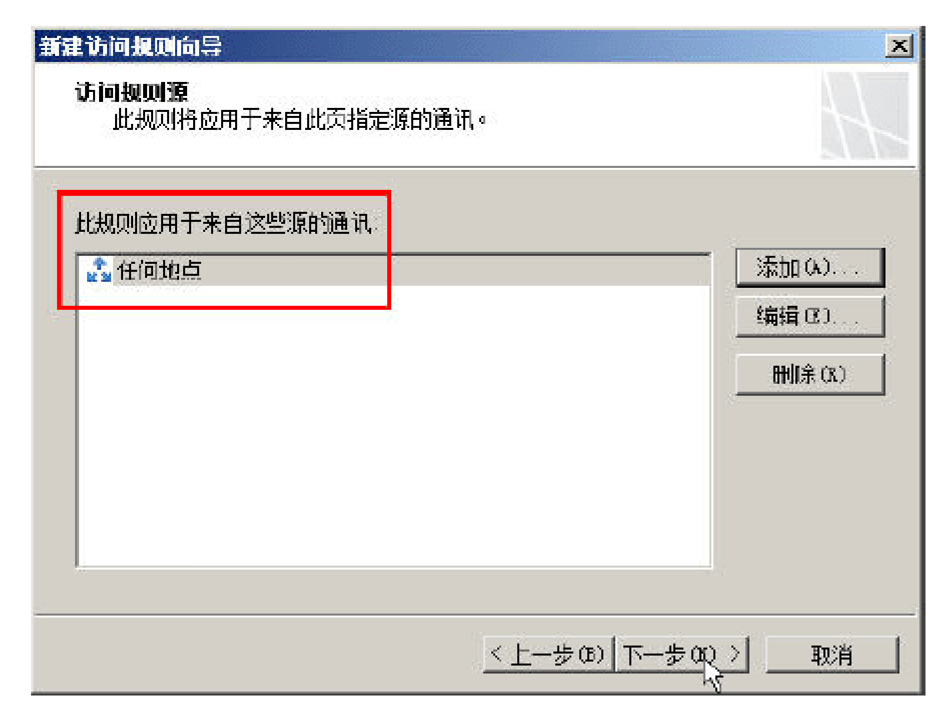


图 16-194 访问规则源

图 16-195 访问规则目标

07 其他选择默认值即可。

08 然后再添加允许“本地主机”以“所有协议”访问“内部”的访问规则。

09 创建完访问规则后，单击“应用”按钮，让设置生效。

16.7.5 为服务器申请证书

在配置好证书服务器后，接下来的工作是为 VPN 服务器申请“服务器证书”并将该证书保存在“计算机存储”中。

申请计算机证书的时候一定要注意，申请的证书的名称要与 VPN 服务器对外提供的名称相同。例如，在本例中，VPN 服务器对外的名称为 sstp.msft.com。

1. 修改 IE 浏览器设置以允许运行 ActiveX 脚本

在第一次从“证书服务器”申请证书时，主要分为 3 个部分：修改 IE 浏览器设置、信任根证

书颁发机构、申请并安装证书。下面分别介绍，首先看“修改 IE 浏览器设置”部分的内容。

01 在 Forefront TMG 计算机上，使用 IE 进入证书申请窗口。在本例中，地址为 http://192.168.254.10/certsrv，如图 16-196 所示。

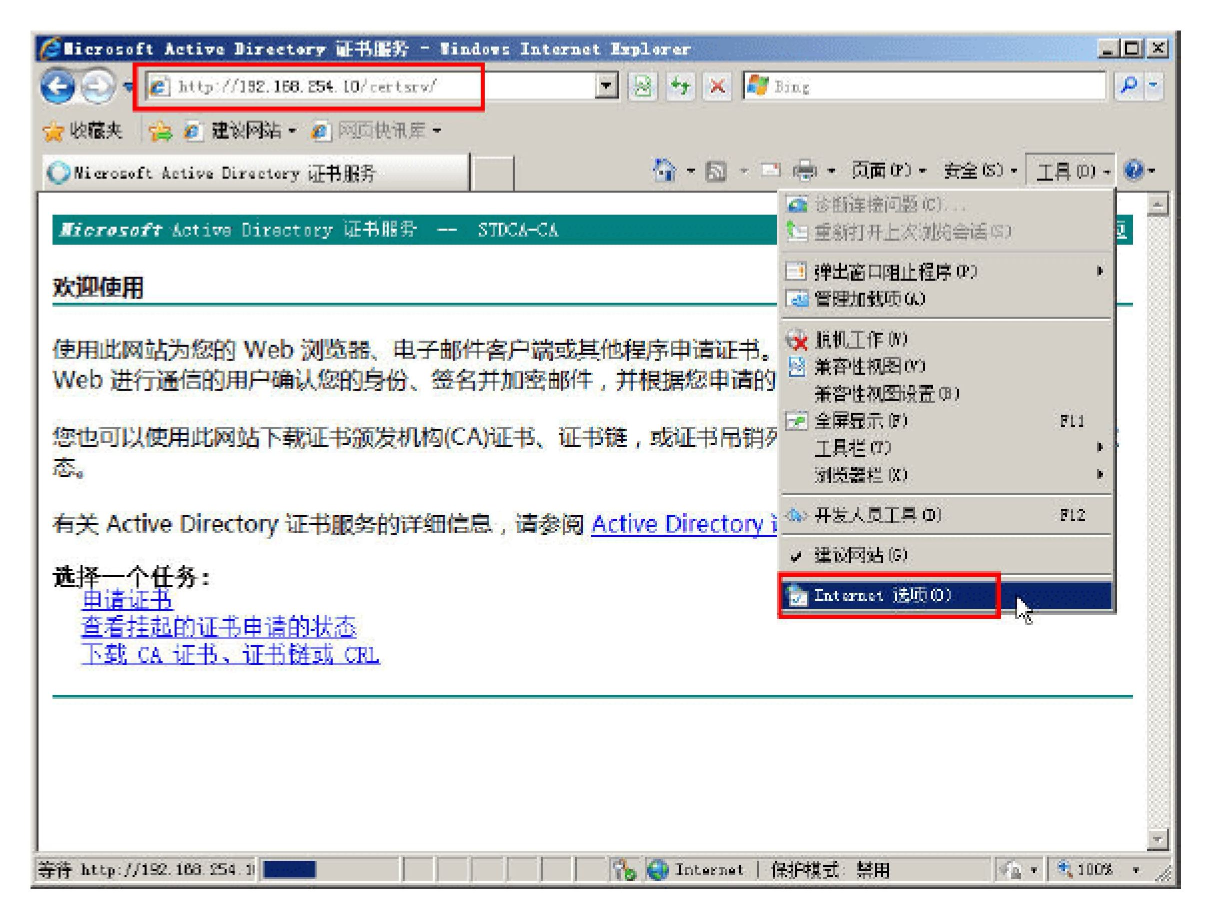


图 16-196 证书申请

02 在申请证书之前，需要修改 IE 的默认设置，允许运行 ActiveX 脚本以从证书服务器申请证书。在“工具”菜单选择“Internet 选项”。为了能从证书服务器申请证书，需要将证书颁发站点添加到“可信站点”图标，并修改安全级别。在“安全”选项卡中，选中“可信站点”图标，单击“站点”按钮，在弹出的“可信站点”对话框中，将 http://192.168.254.10 添加到列表中，并取消选中“对该区域中的所有站点要求服务器验证”复选框，如图 16-197 所示。

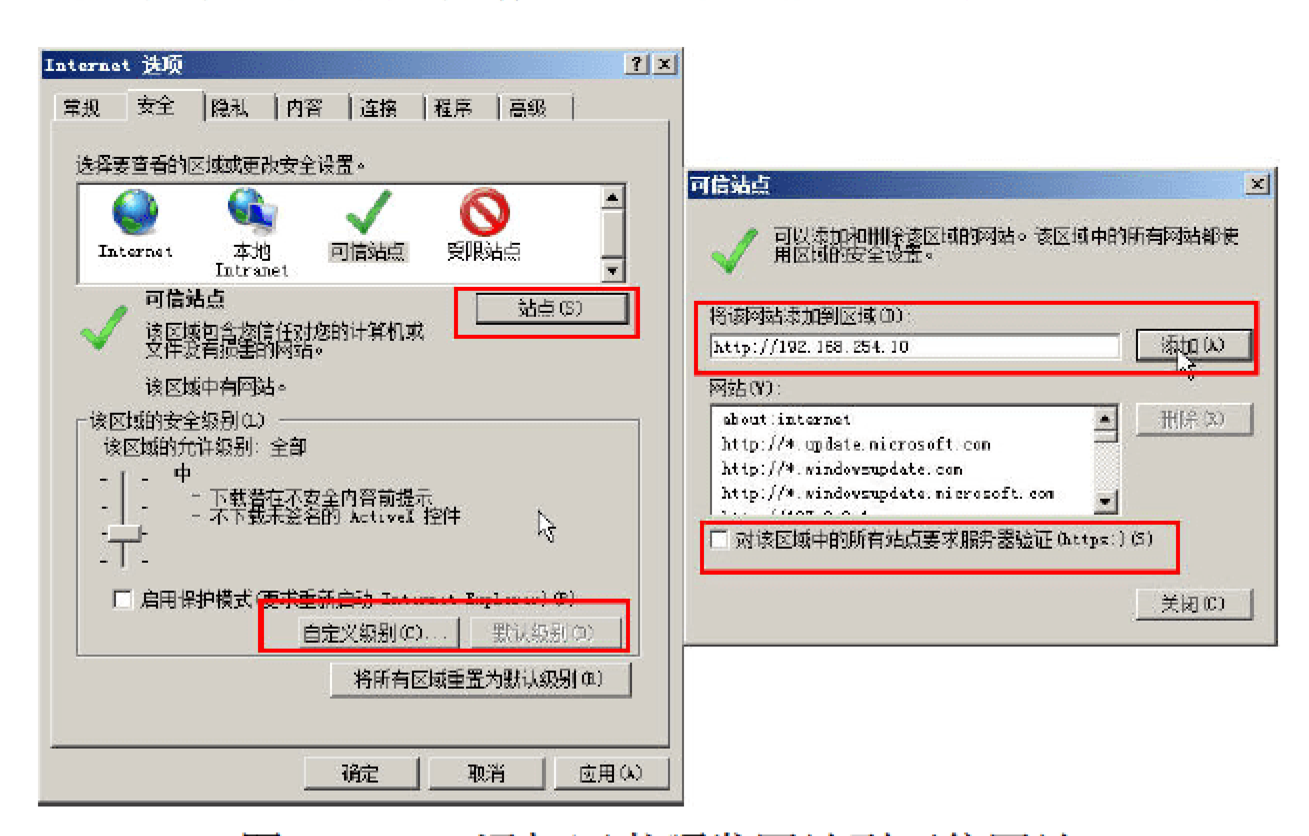


图 16-197 添加证书颁发网站到可信网站

03 添加可信站点之后，单击“关闭”按钮返回到“安全”选项卡，并单击“自定义级别”按钮（如果“自定义级别”按钮不可用，请先单击“默认级别”按钮），在弹出的“安全设置-受信任的站点区域”对话框中，在“ActiveX 控件和插件”选项中，须 “启用”各个选项，这包括“ActiveX 控件自动提示”、“对标记为可安全执行脚本的 ActiveX 控件执行脚本”、“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行”、“二进制脚本行为”、“下载未签名的 ActiveX 控件”、“下载已签名的 ActiveX 控件”、“允许 Scriptlet”、“允许运行以前未使用的 ActiveX

而不提示”、“运行 ActiveX 控件和插件”等，如图 16-198 所示。设置完成之后，单击“确定”按钮，在弹出的“警告”对话框中，单击“是”按钮，如图 16-199 所示。

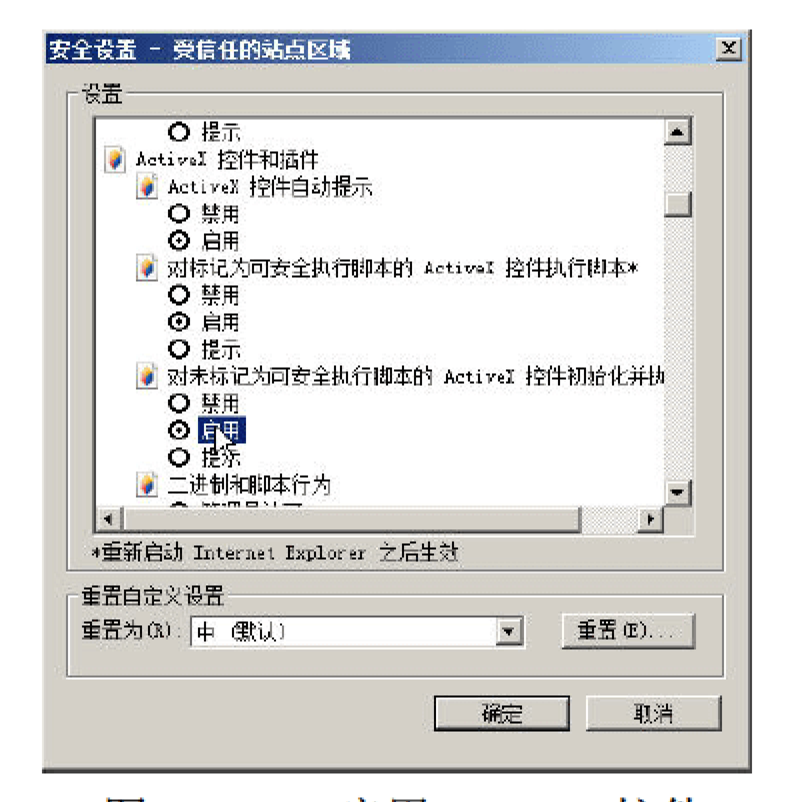


图 16-198　启用 ActiveX 控件



图 16-199　更改区域

2 信任根证书颁发机构

接下来的操作，是“信任”根证书颁发机构。一般的方法是下载根书并导入“本地计算机→受信任的根证书颁发机构”中，本文介绍另一种方法。

01 设置完成之后，返回到证书申请窗口，单击“下载 CA 证书、证书链或 CRL”链接，进入“下载 CA 证书、证书链或 CRL”对话框，单击“下载 CA 证书”链接，在弹出的对话框中单击“打开”按钮，如图 16-200 所示。

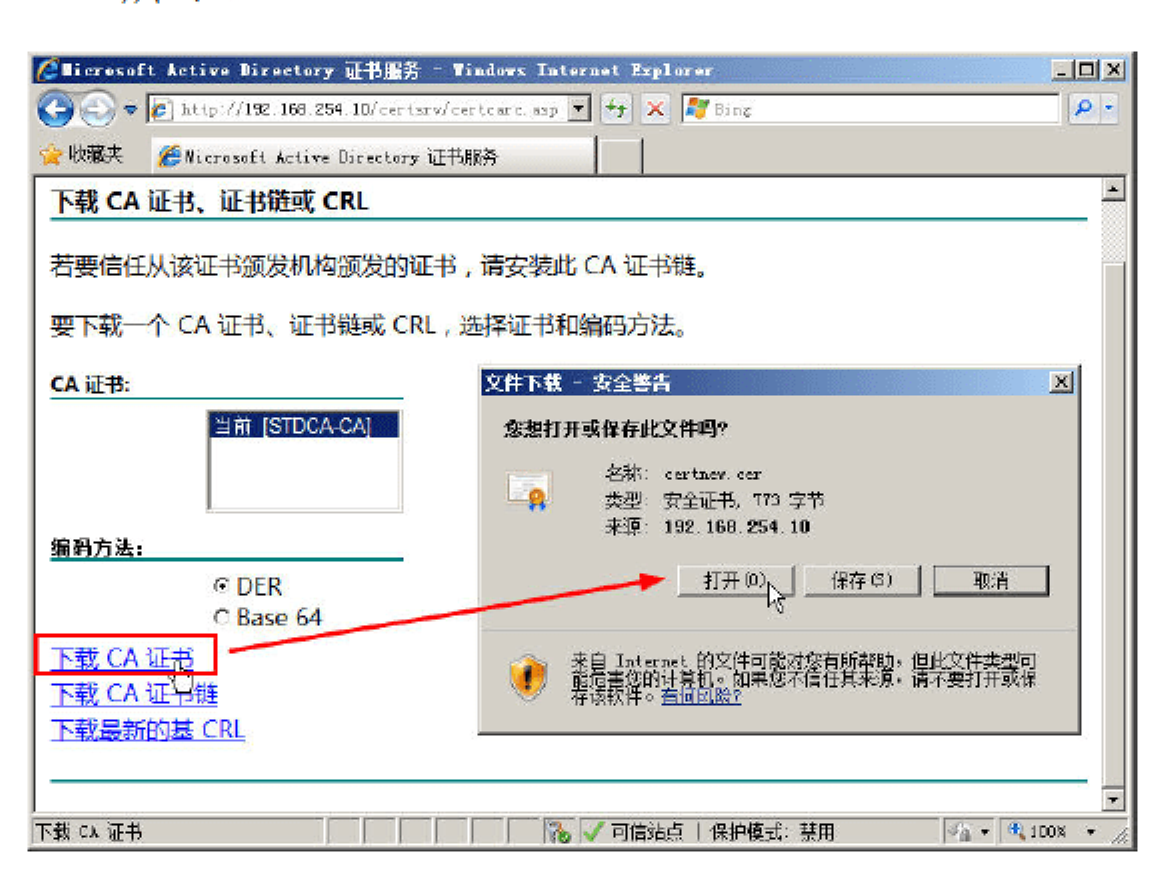


图 16-200　打开证书

02 在弹出的“证书”对话框中可以看到，当前 CA 根证书不受信任，如图 16-201 所示，单击“安装证书”按钮。

03 在“欢迎使用证书导入向导”对话框中，单击“下一步”按钮，如图 16-202 所示。

04 在“证书存储”对话框中，选中“将所有的证书放入下列存储”单选按钮，单击“浏览”按钮，在弹出的“选择证书存储”对话框中，选中“显示物理存储区”复选框，然后在“选择要使用的证书存储”列表框中选择“受信任的根证书颁发机构→本地计算机”，如图 16-203 所示。

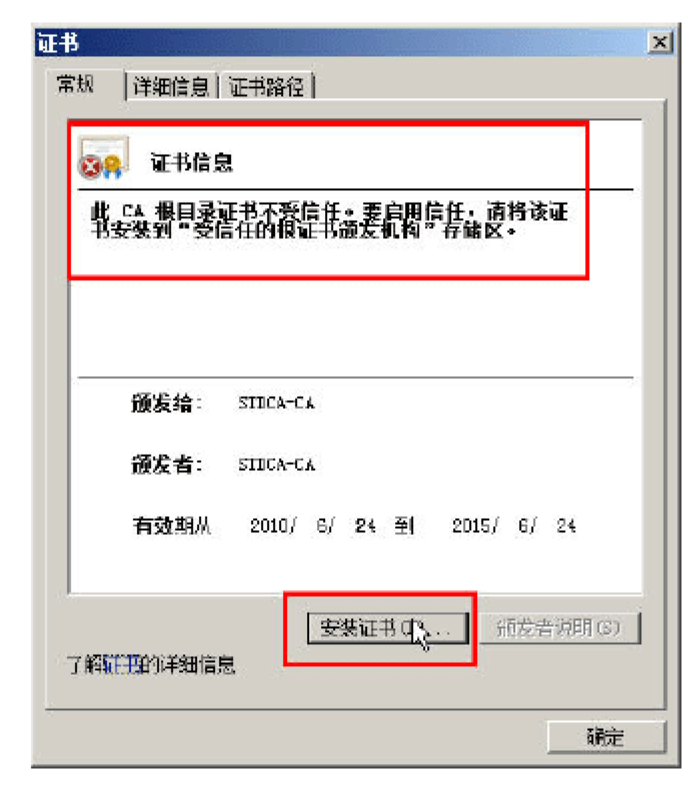


图 16-201　安装证书

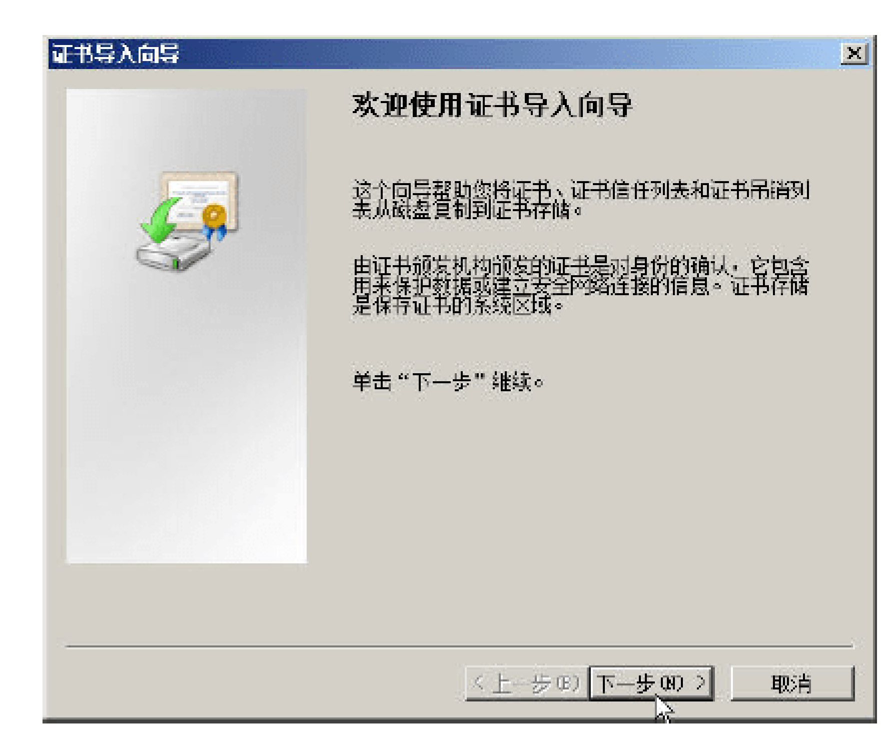


图 16-202　证书导入向导

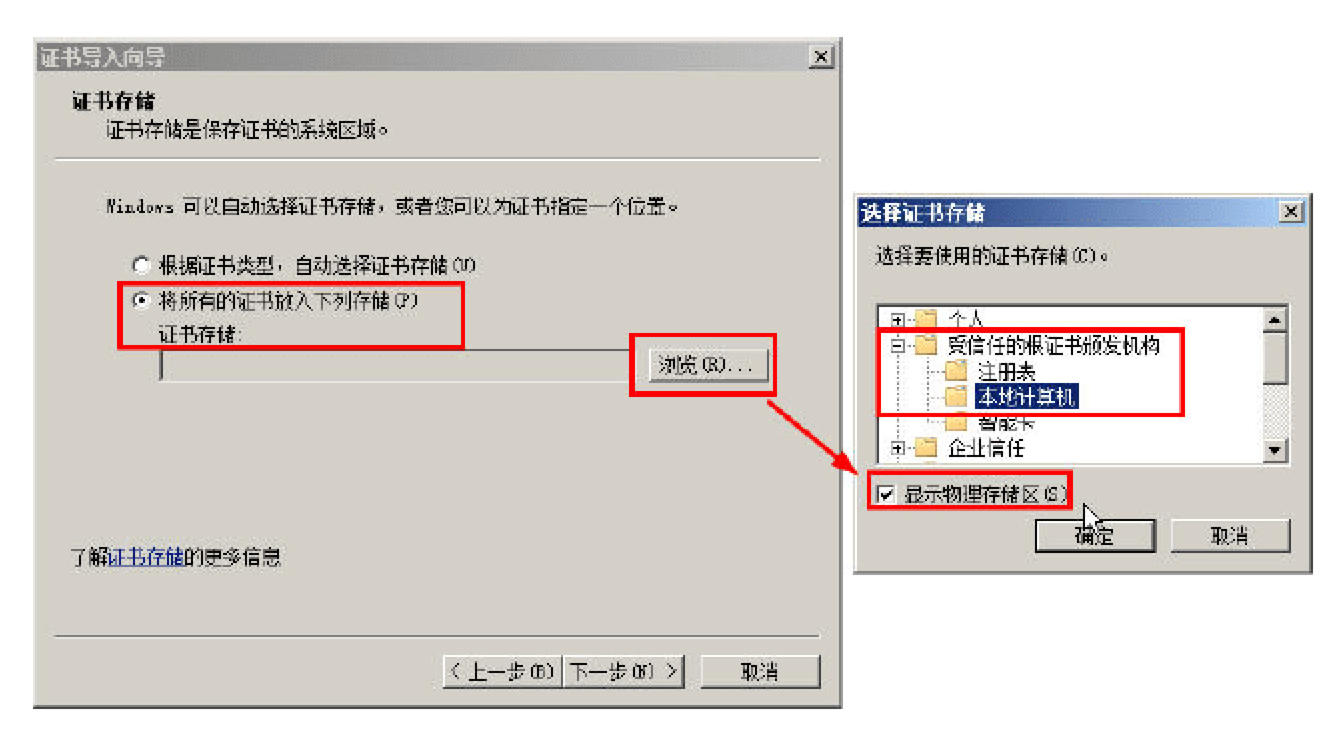


图 16-203　保存在计算机存储中

05 在“正在完成证书导入向导”对话框中，单击“完成”按钮，如图 16-204 所示。



图 16-204　完成证书导入向导

3. 申请服务器证书

在“信任根证书颁发机构”之后，就可以申请“服务器证书”了，接下来将申请名为“sstp.msft.com”的服务器证书，并且在申请证书的时候要“标记密钥为可导出”。申请的主要步骤如下。

01 在证书申请网站（本例为 http://192.168.254.10/certsrv），返回到证书申请窗口，单击“申请证书”链接，如图 16-205 所示。

02 在“申请一个证书”窗口，单击“高级证书申请”链接，如图 16-206 所示。




图 16-205　申请证书

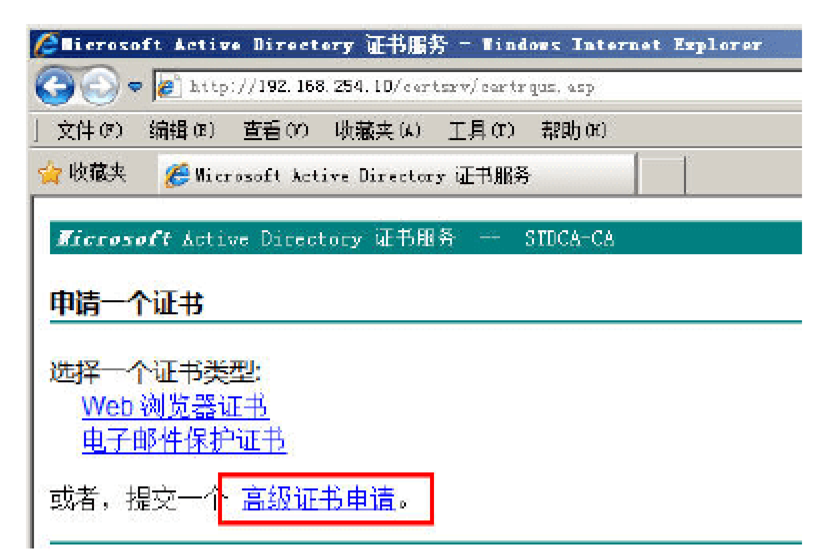


图 16-206　高级证书申请

03 在“高级证书申请”窗口，单击“创建并向此 CA 提交一个申请”链接，如图 16-207 所示。

04 申请证书的时候，有 3 个关键点：证书的名称要与 Forefront TMG 对外显示的名称一致、证书类型选择“服务器身份验证证书”选项、选中“标记密钥为可导出”复选框，如图 16-208 所示。其他可以随意设置。

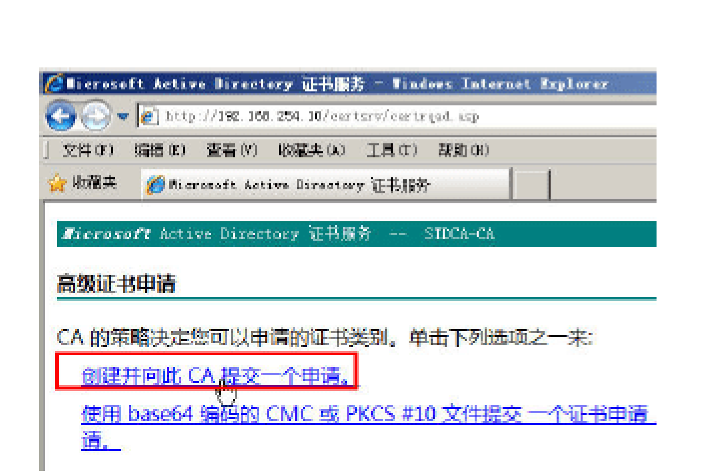


图 16-207　申请证书

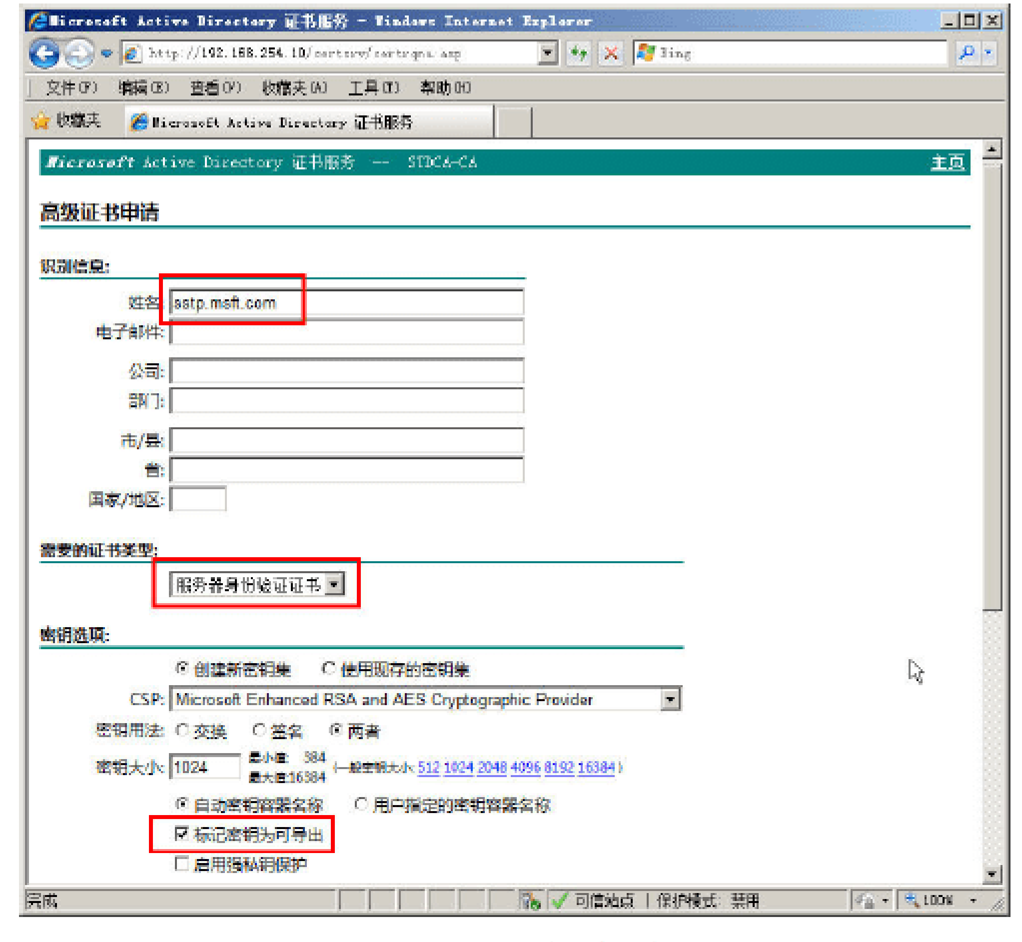


图 16-208　证书申请页

05 如果在证书服务器的属性对话框中，设置了自动颁发证书，则会提示“证书已颁发”，单击“安装此证书”链接，即可安装证书，如图 16-209 所示。

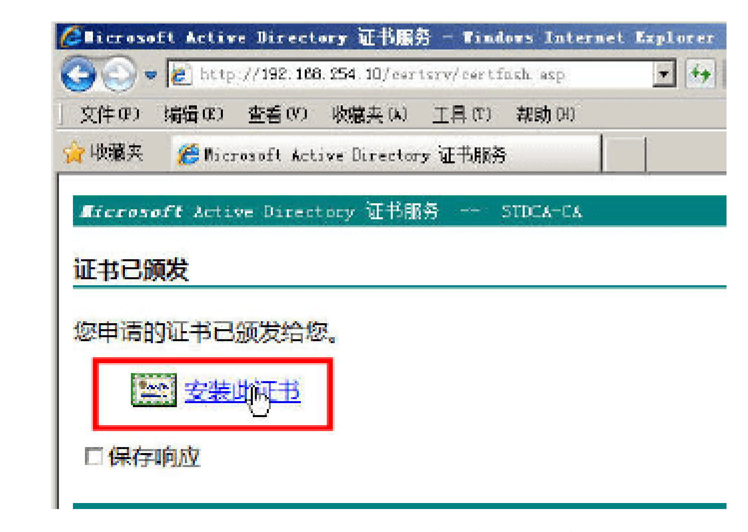


图 16-209　安装证书

4. 在 Windows 2008 中导出用户证书并导入到计算机存储中

在安装完证书之后，还需要将证书从“用户存储”中导出，然后导入到“计算机存储”中，才能为 VPN 服务器使用。在本例中，我们将使用 MMC 控制台，通过添加用户与计算机证书的方式，完成这一过程。

01 运行 MMC，添加两次“证书”管理工具，在添加的时候，分别添加“当前用户”与“本地计算机”，然后定位到“证书-当前用户→个人→证书”节，在右侧窗格选中已经安装的 sstp.msft.com 证书，单击鼠标右键，在弹出的快捷菜单中选择“所有任务→导出”命令，如图 16-210 所示。

02 在“导出私钥”对话框中，选中“是，导出私钥”单选按钮，如图 16-211 所示。

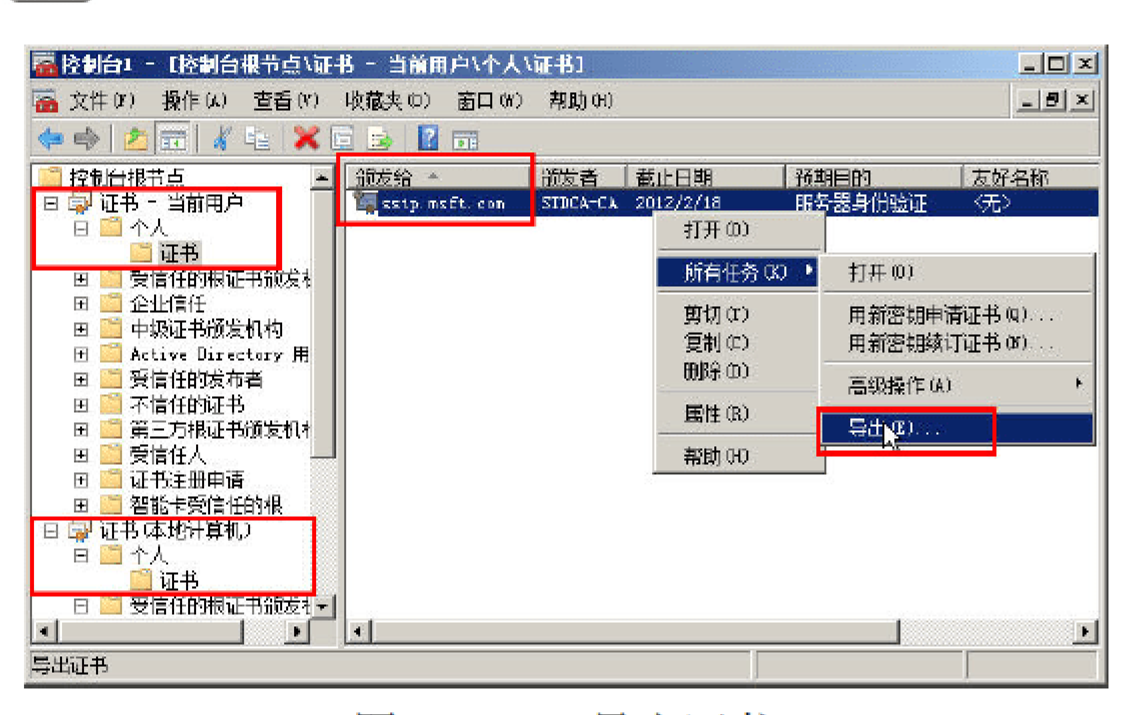


图 16-210 导出证书

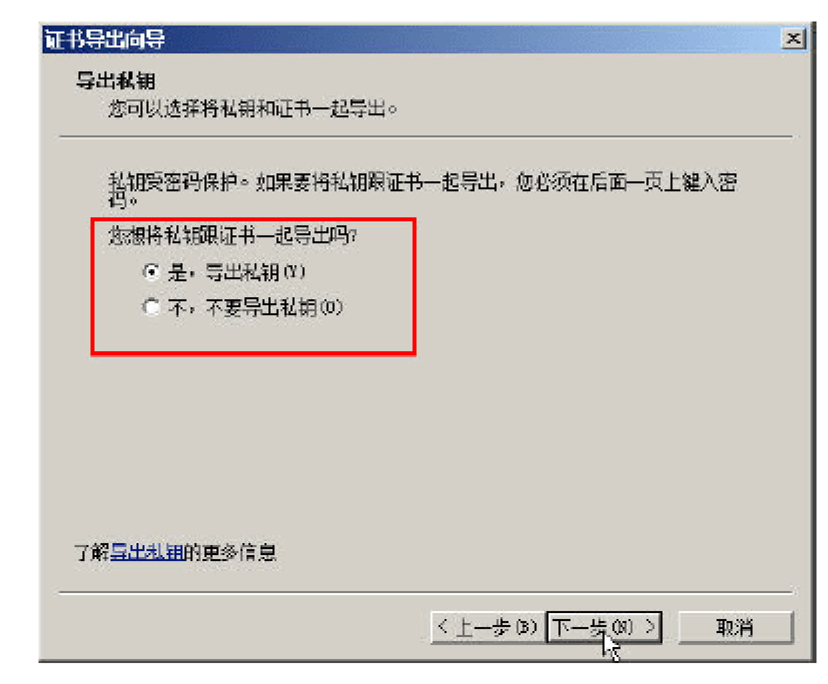


图 16-211 导出私钥

03 在“导出文件格式”对话框中，选中“如果导出成功，删除私钥”复选框，如图 16-212 所示。这样，可以防止他人再导出证书。

04 在“密码”对话框中设置密码，用来保护导出的私钥，如图 16-213 所示。

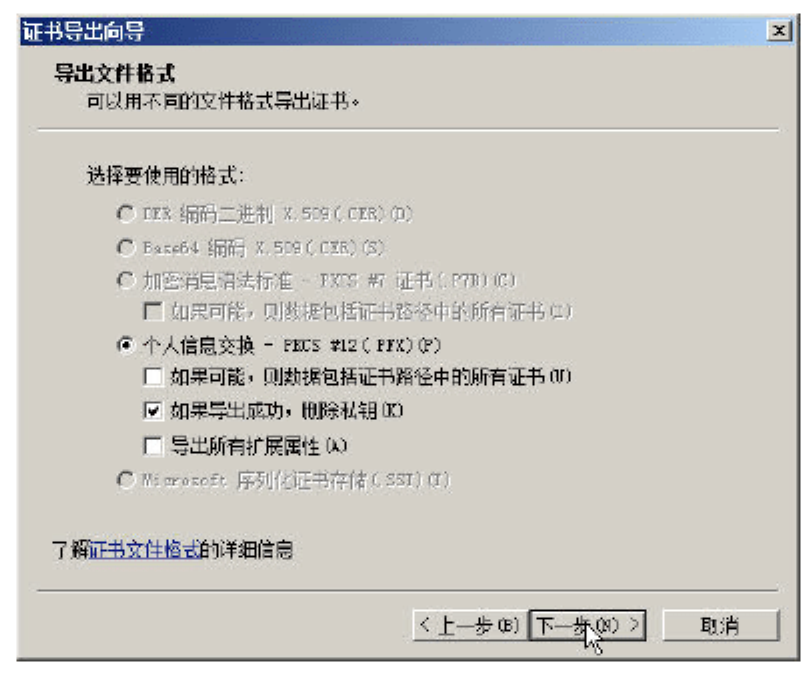


图 16-212 导出成功删除密钥

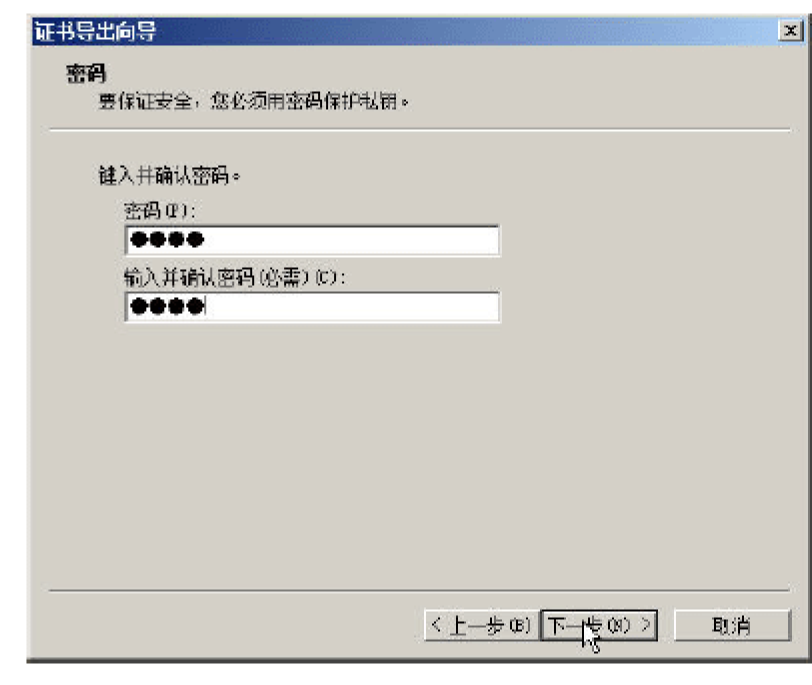


图 16-213 设置保护密码

05 在“要导出的文件”对话框中，单击“浏览”按钮，为导出的证书设置保存的路径与保存文件名，如图 16-214 所示。在本例中，将证书导出到“桌面”，并设置保存文件名为 sstp.pfx。

06 导出成功后，单击“完成”按钮，如图 16-215 所示。

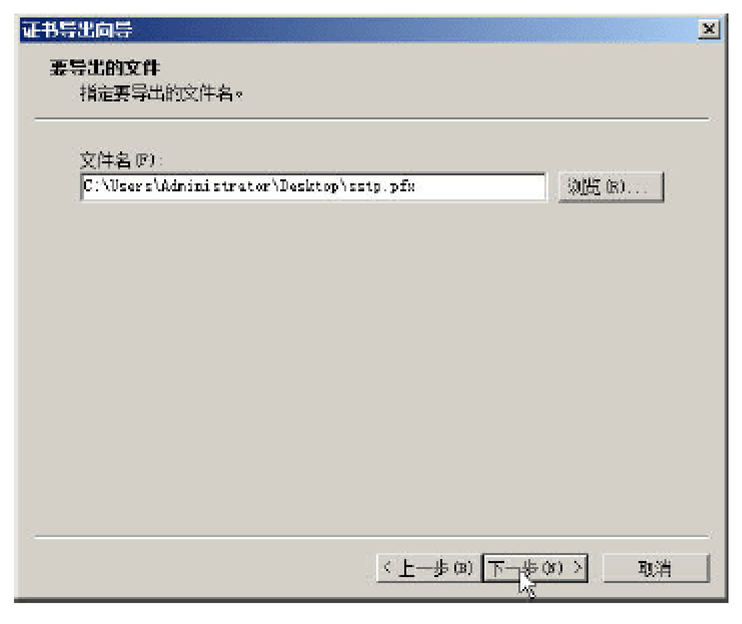


图 16-214 设置保存文件名

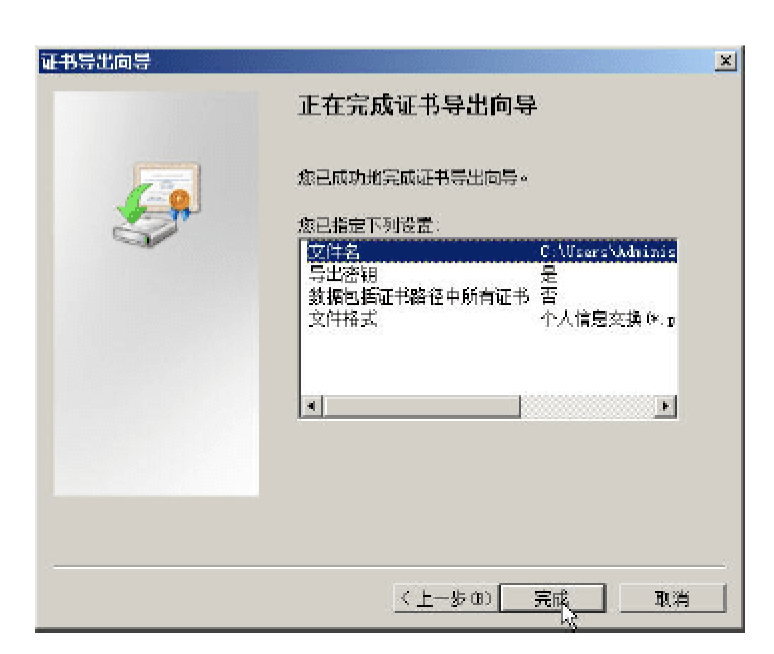


图 16-215 导出成功

07 导出证书完成之后，返回到控制台，定位到“证书→个人→证书”，在右侧的空白窗格中用鼠标右键单击，从弹出的快捷菜单中选择“所有任务→导入”命令，如图 16-216 所示。

08 在“证书导入向导→要导入的文件”对话框中，选择前面导出的证书文件，如图 16-217 所示。

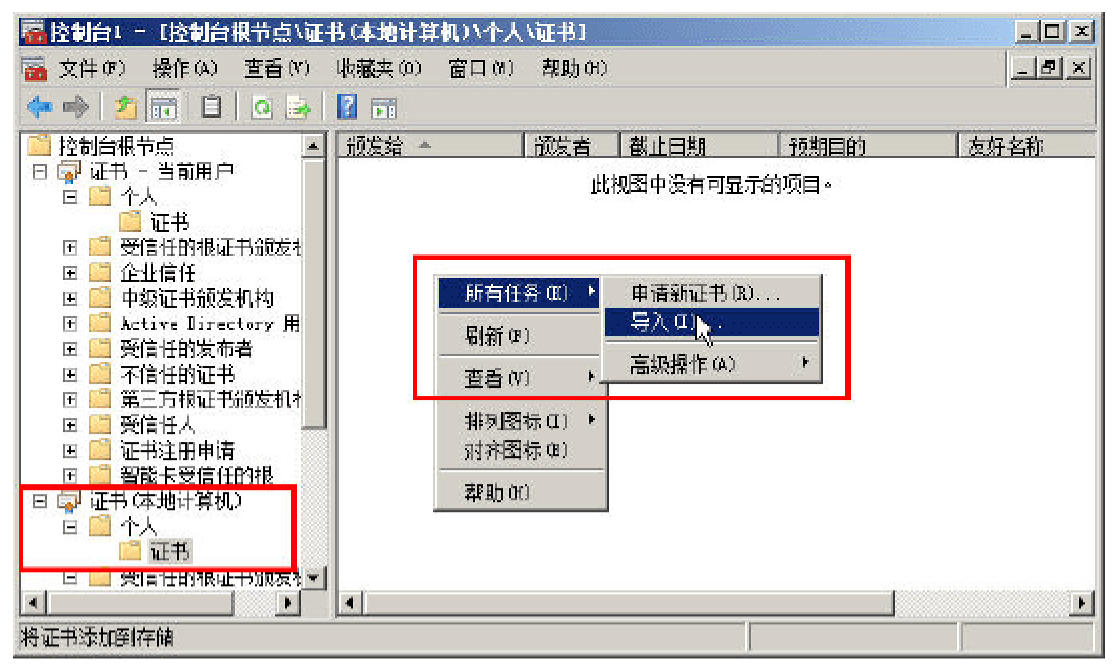


图 16-216　导入证书

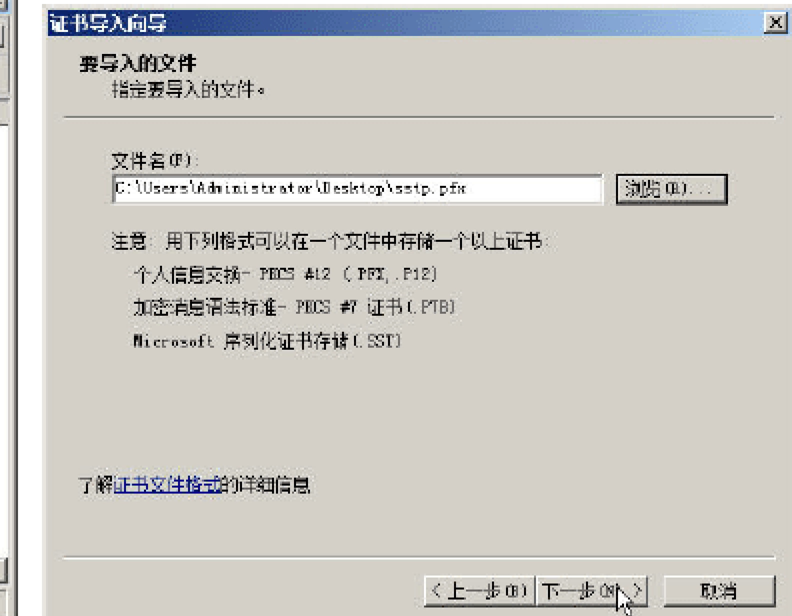


图 16-217　选择要导入的证书

09 在“密码”对话框中，输入保护私钥的密码，如图 16-218 所示。

10 在“证书存储”对话框中，选择默认值。

11 导入成功之后，单击“完成”按钮，如图 16-219 所示。

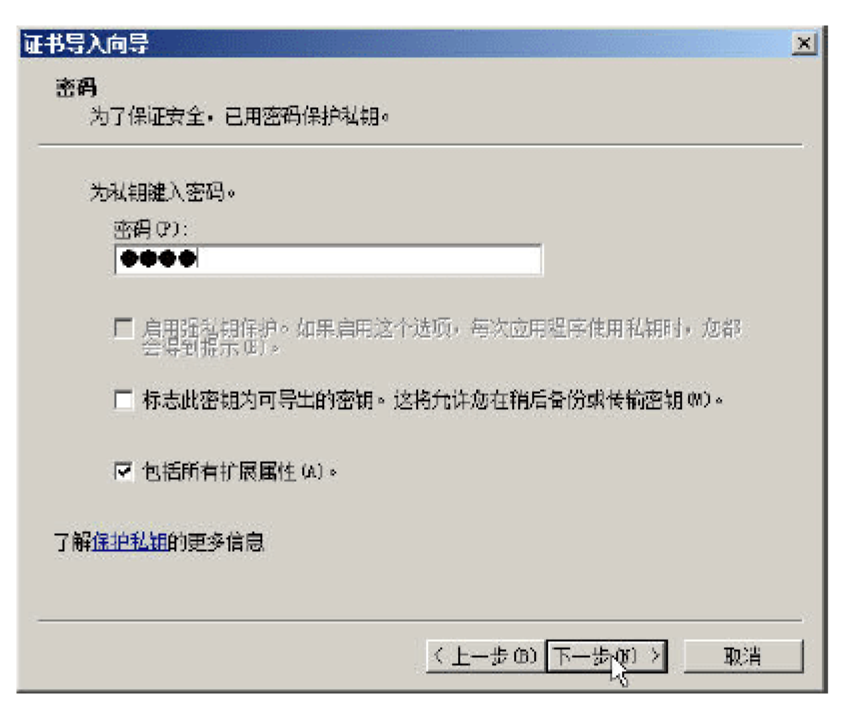


图 16-218　输入保护密码

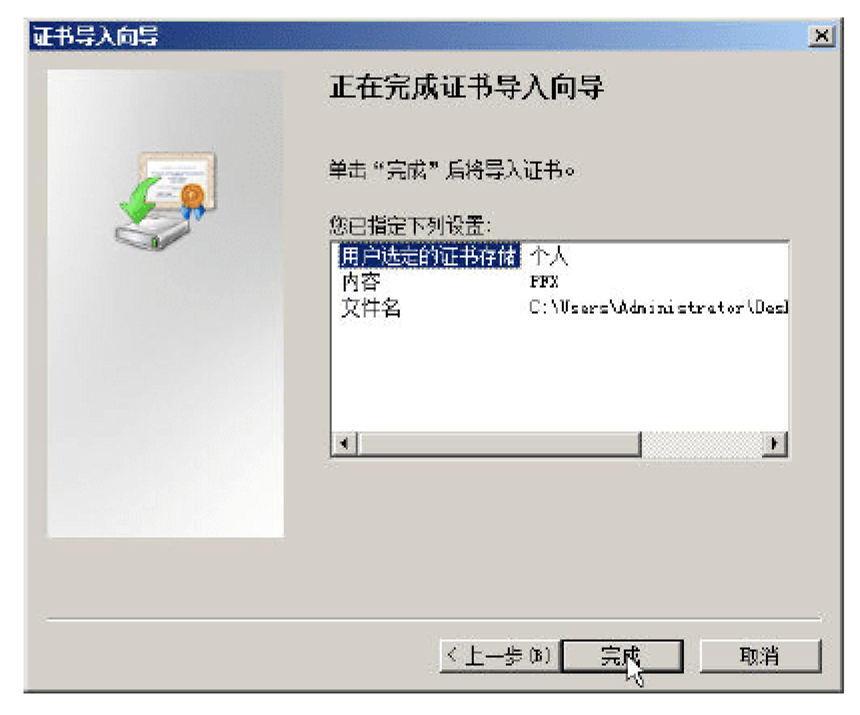


图 16-219　导入完成

16.7.6　配置 Forefront TMG 使用 SSTP 协议

在配置 Forefront TMG 使用 SSTP 协议之前，还需要创建一个使用 SSL 协议的“Web 侦听器”，并且“Web 侦听器”绑定的证书是前文申请并导入到“计算机存储”中的证书。创建“Web 侦听器”的主要步骤如下。

01 定位到 Forefront TMG 的“防火墙策略”中，在右侧窗格的“工具箱”选项卡中，在“网络对象”中单击“新建”按钮，在下拉菜单中选择“Web 侦听器”命令，如图 16-220 所示。

02 在“欢迎使用新建 Web 侦听器向导”对话框中，设置一个名称，在此为 SSTP VPN，如图 16-221 所示。

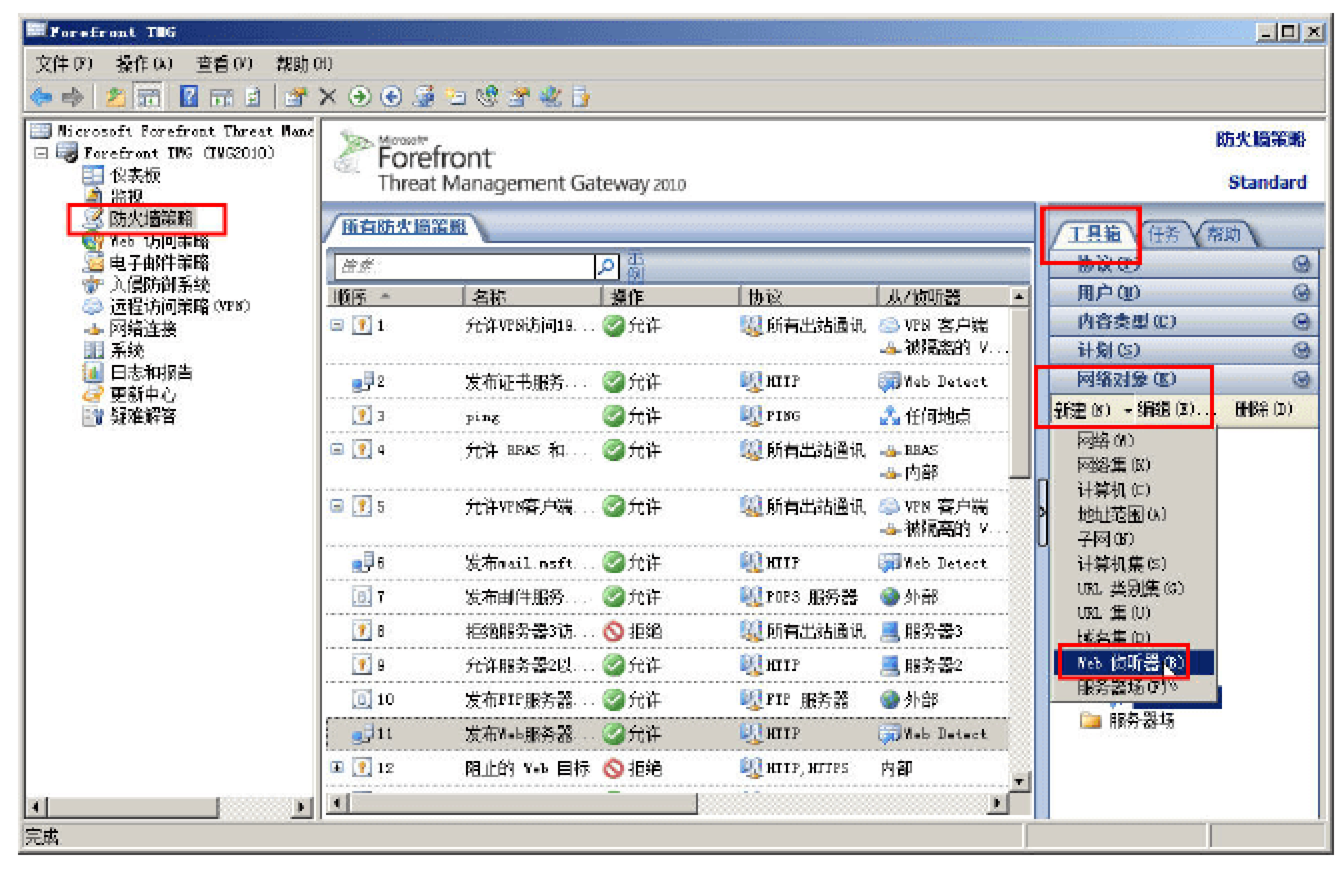


图 16-220 新建 Web 侦听器

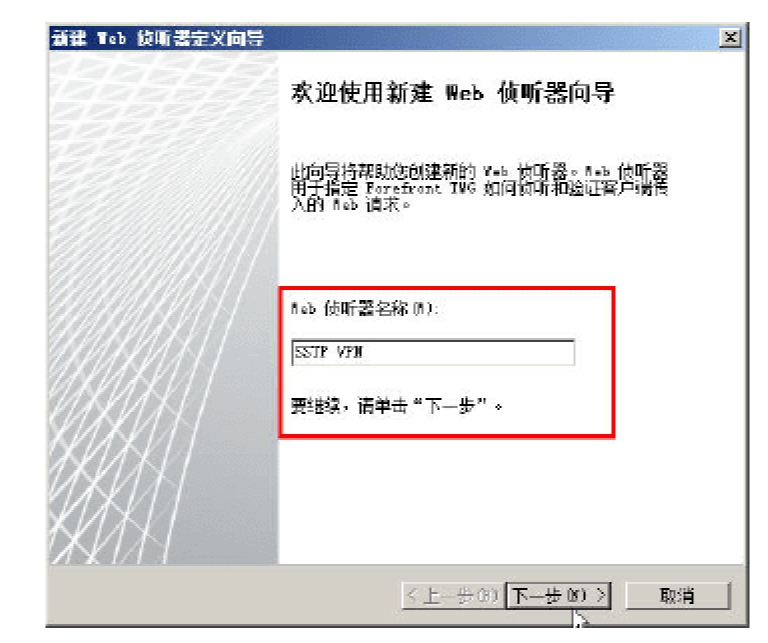


图 16-221 为 Web 侦听器设置名称

03 在“客户端连接安全设置”对话框中，选中“需要与客户端建立 SSL 安全连接”单选按钮，如图 16-222 所示。

04 在“Web 侦听器 IP 地址”对话框中，选中“外部”复选框，如图 16-223 所示。

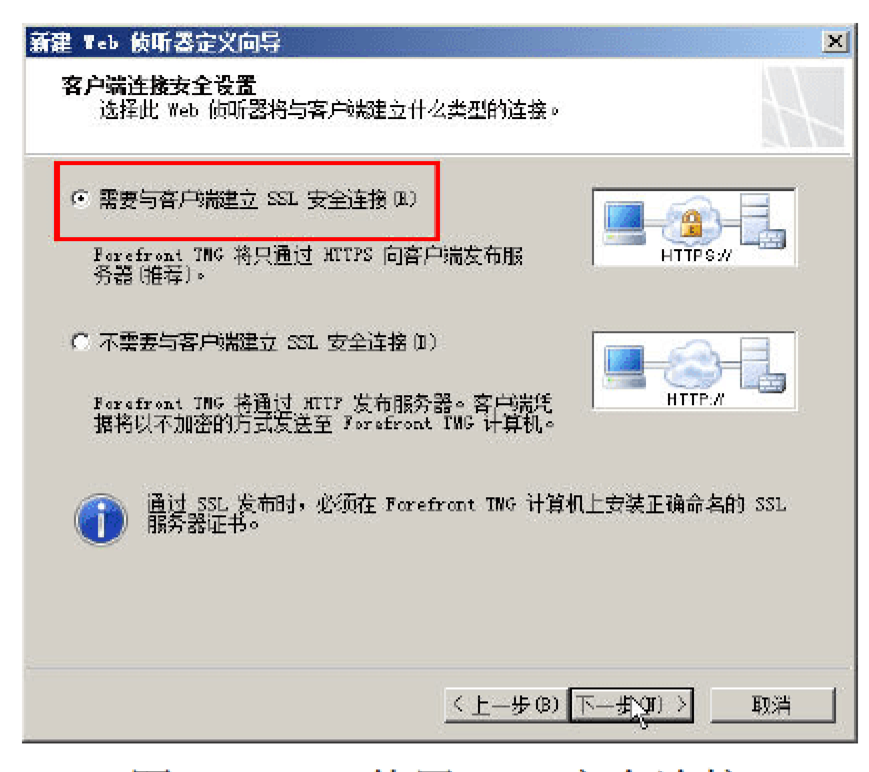




图 16-222 使用 SSL 安全连接

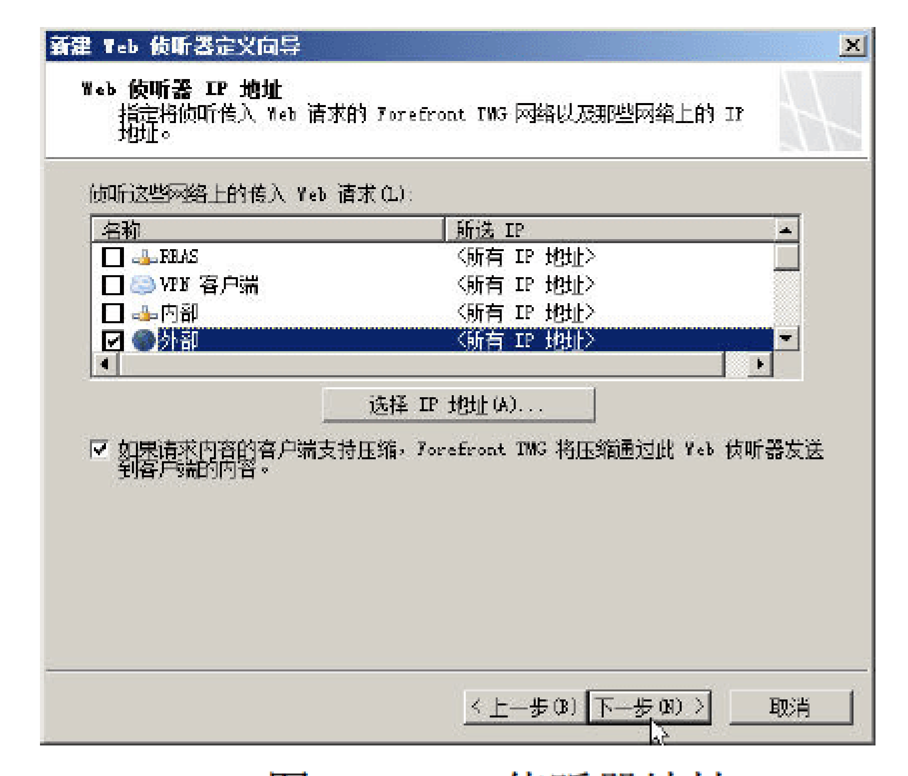


图 16-223 侦听器地址

05 在“侦听器 SSL 证书”对话框中，单击“选择证书”按钮，在弹出的“选择证书”对话框中选择前文安装的证书，如图 16-224 所示。

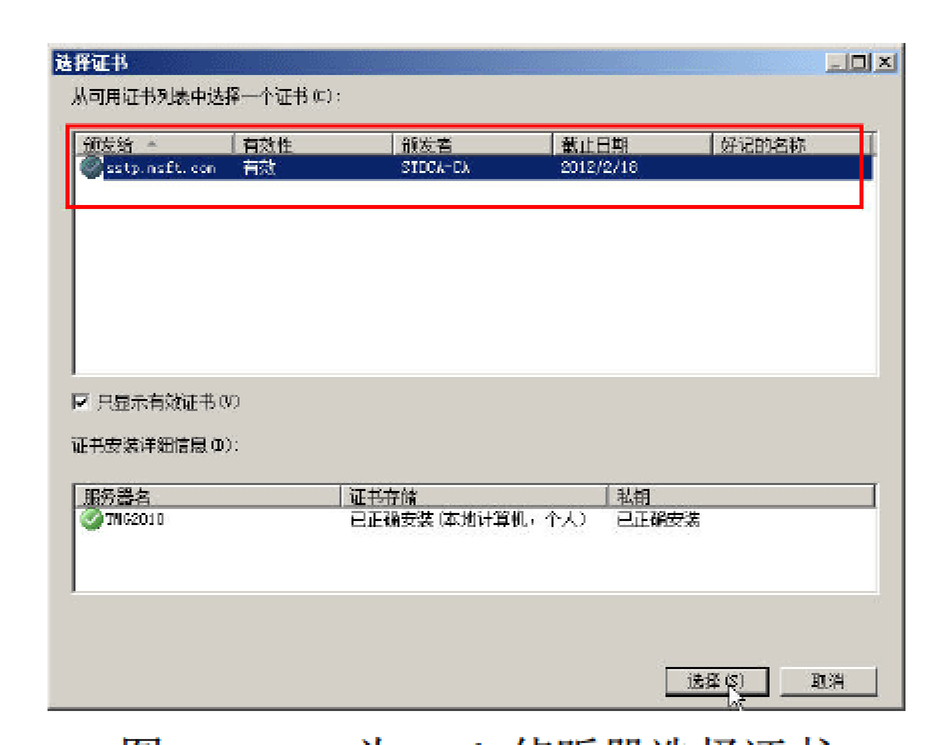


图 16-224 为 Web 侦听器选择证书

06 其他选择默认值。

在创建好 SSL Web 侦听器后，配置 VPN 服务器，为 VPN 服务器选择 SSTP 协议并选择 SSL Web 侦听器，主要步骤如下。

01 在 Forefront TMG 控制台中，定位到“远程访问策略（VPN）”1 节，选中“VPN 客户端”，在“任务”选项卡中单击“配置 VPN 客户端访问”链接，如图 16-225 所示。

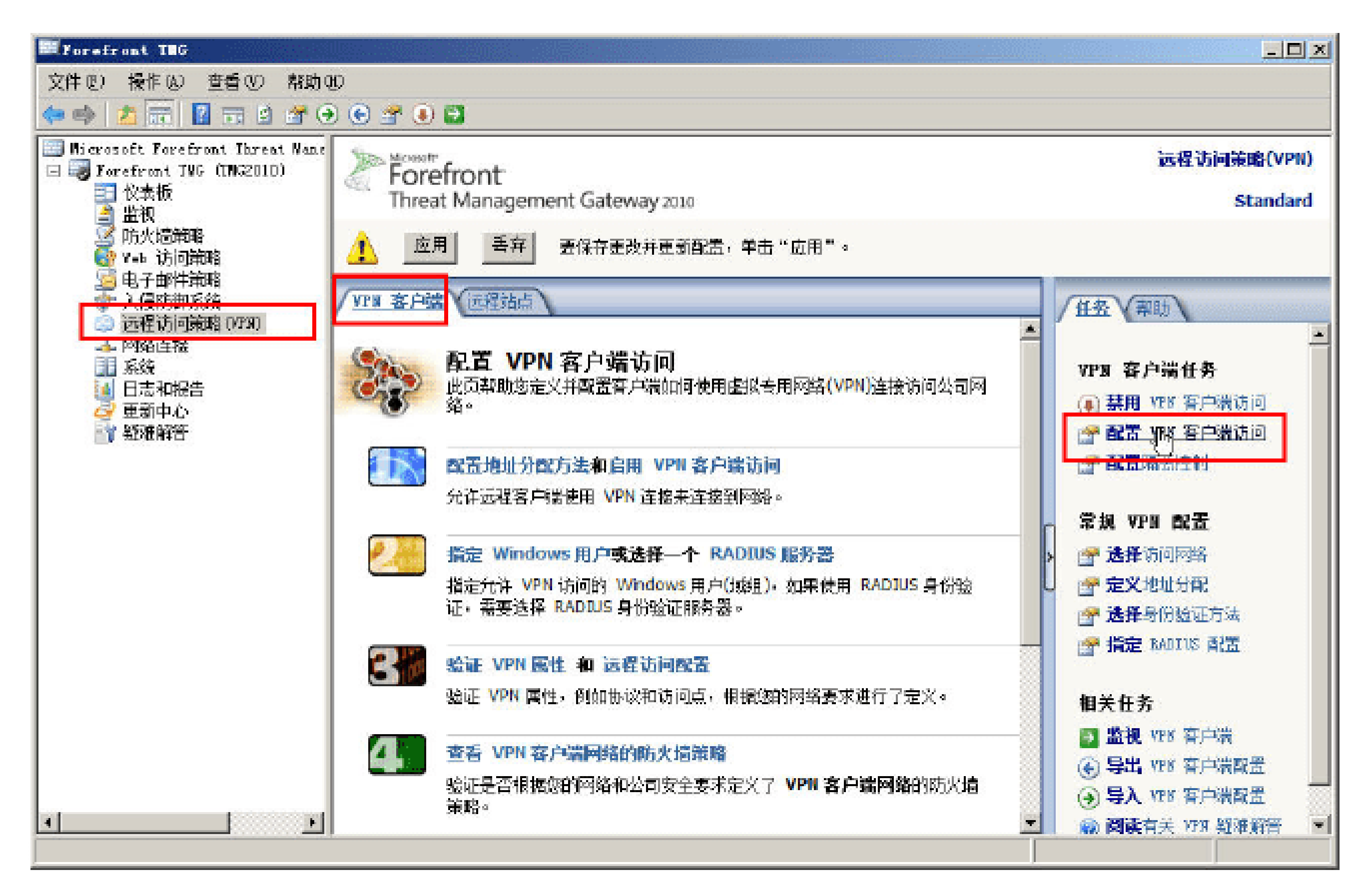


图 16-225　配置 VPN 客户端访问



说 明

需要提前将 Forefront TMG 配置为 VPN 服务器，有关这些操作，可参见“16.5.1 在 Forefront TMG 中启用 VPN 服务器”一节内容。

02 在“VPN 客户端 属性”对话框中，在“协议”选项卡中，选中“启用 SSTP”复选框，并单击“选择侦听器”按钮，在弹出的“为 SSTP 选择 Web 侦听器”对话框中，选择“SSTP VPN”选项，如图 16-226 所示，并单击“确定”按钮，返回到“VPN 客户端 属性”对话框，再次单击“确定”按钮，完成设置。

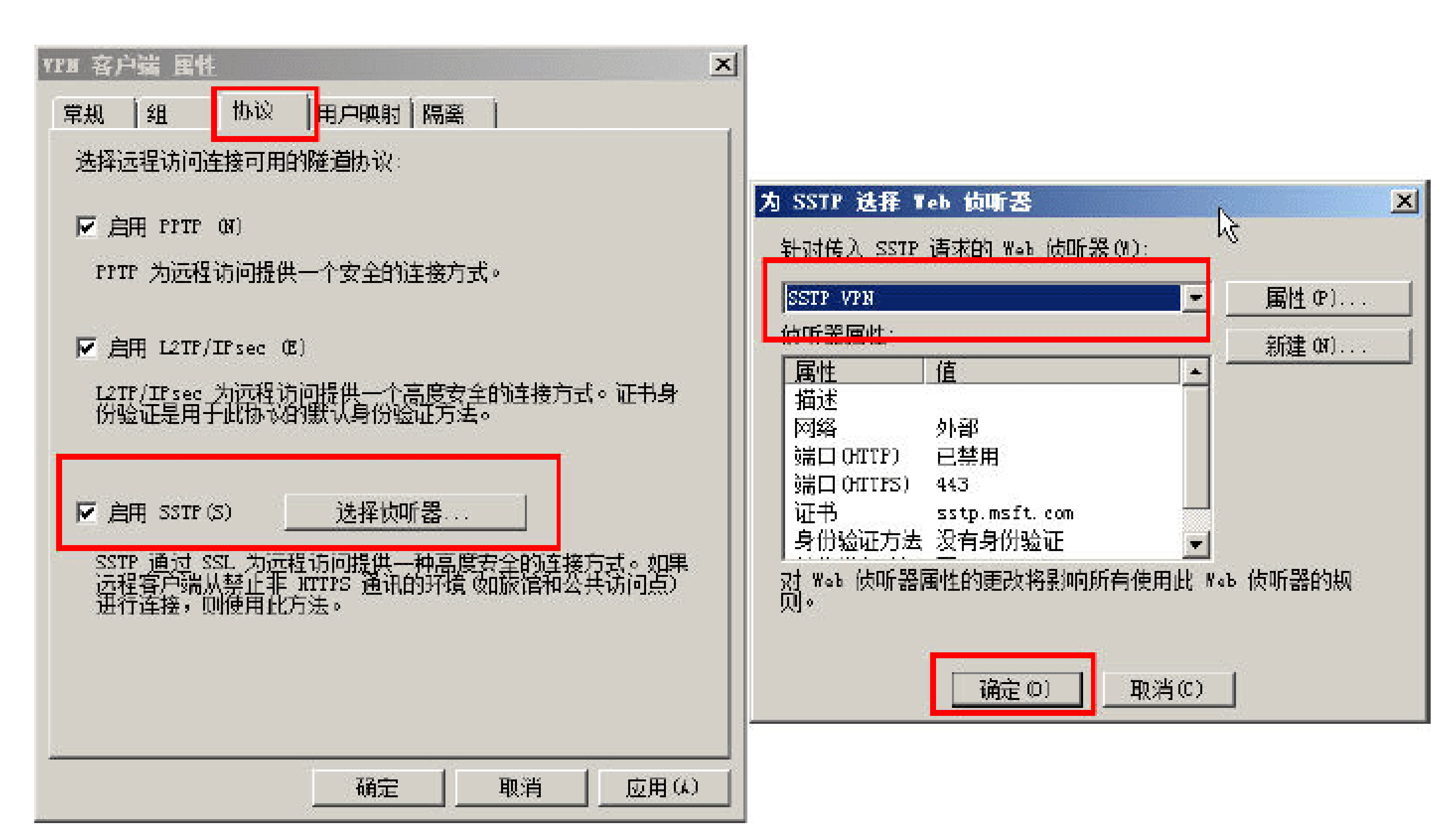


图 16-226　启用 SSTP 协议

设置完成后，单击“应用”按钮，让设置生效，如图 16-227 所示。

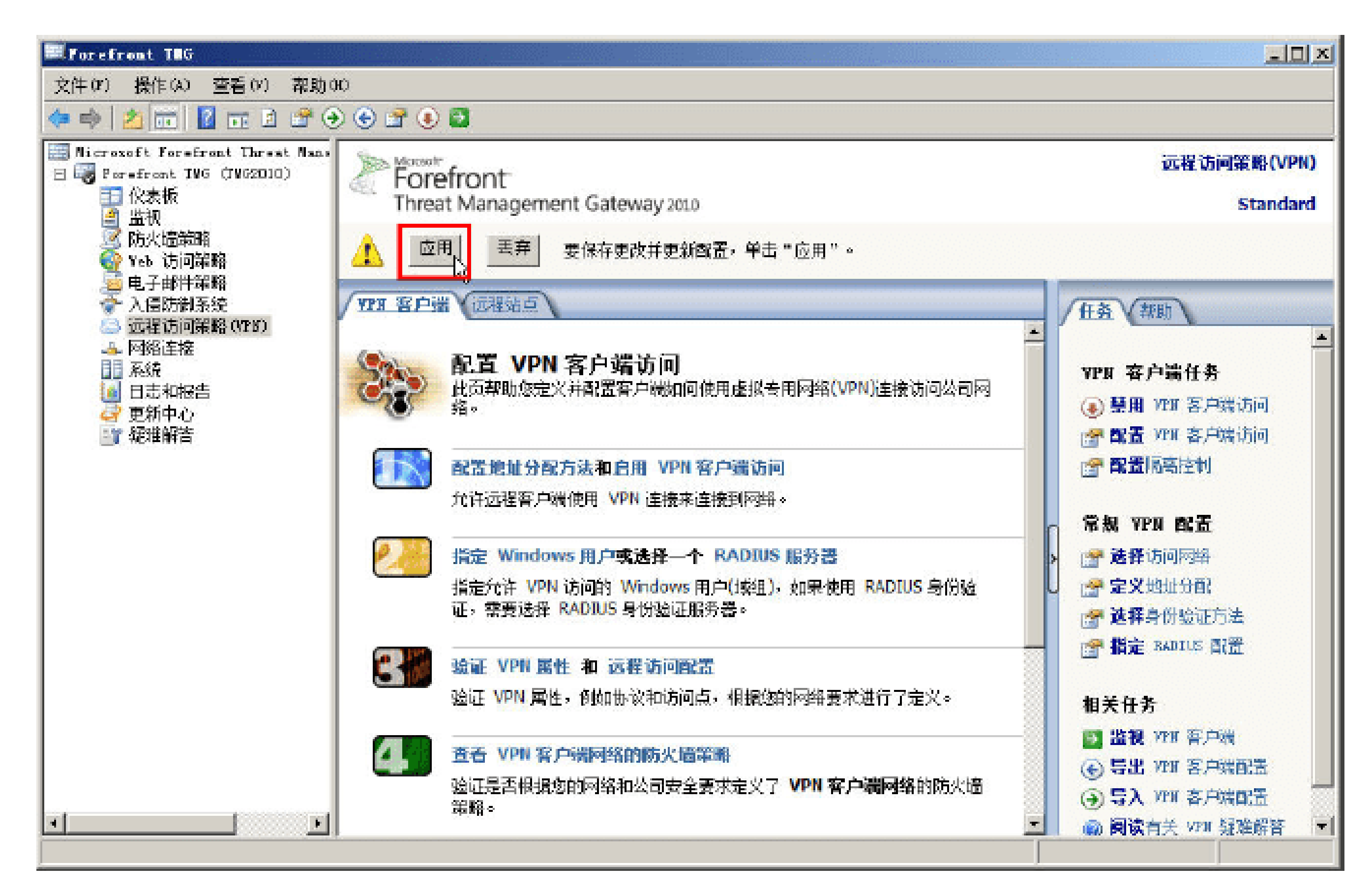


图 16-227　让设置生效

16.7.7　修改 NPS 访问策略

在使用 Forefront TMG 配置 SSTP VPN 服务器的时候，需要修改 NPS 策略，步骤如下.

01 在“服务器管理器”中，定位到“角色→网络策略和访问服务→NPS（本地）→策略→连接请求策略”节，在中间窗格用鼠标右击“Microsoft 路由和远程访问服务策略”，在弹出的快捷菜单中选择“属性”命令，如图 16-228 所示。

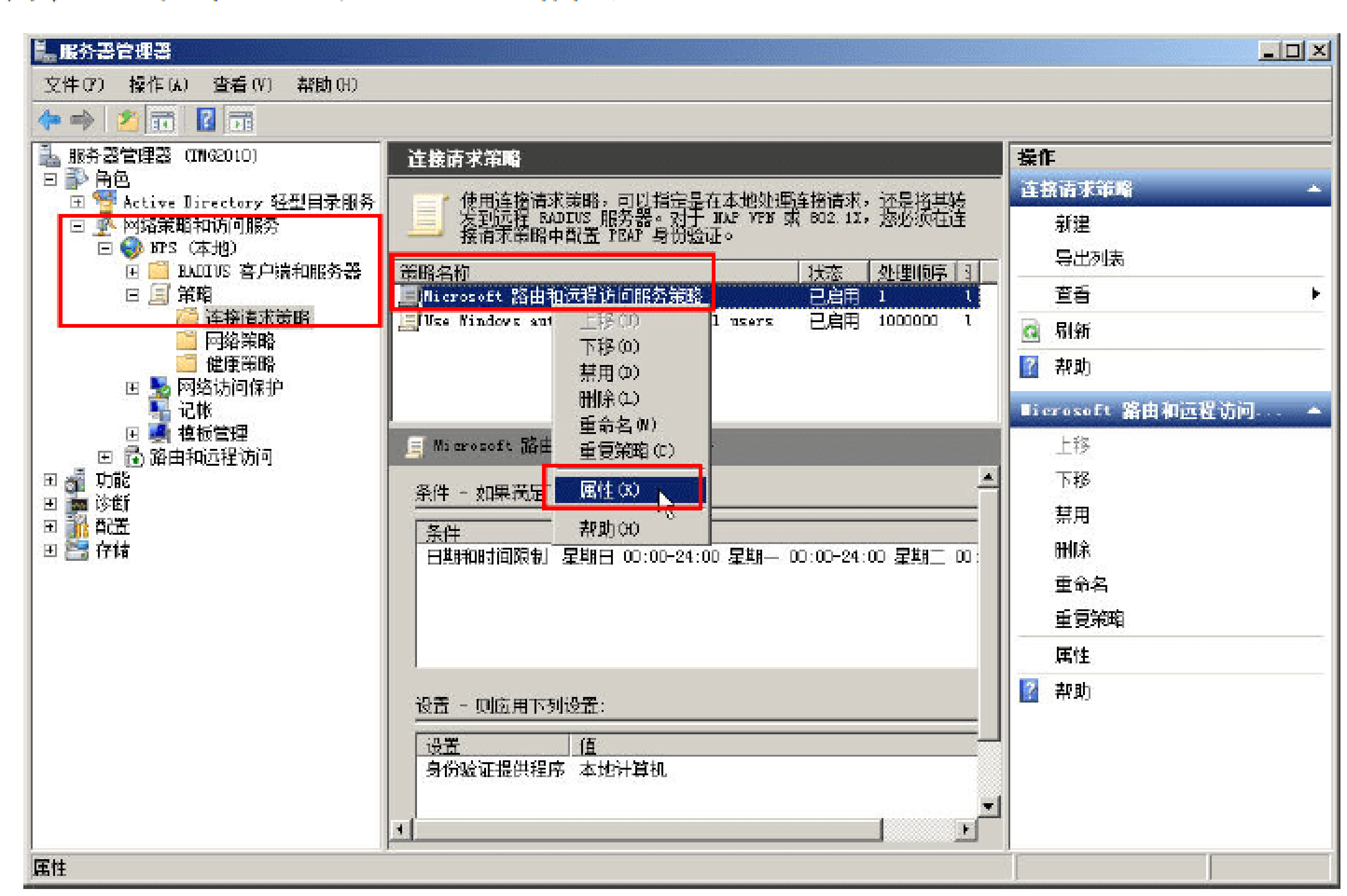


图 16-228　属性

02 在“Microsoft 路由和远程访问服务策略 属性”对话框中，单击“设置”选项卡，在“身份验证方法”一节，选中“改写网络策略身份验证设置”复选框，并在“EAP 类型”列表中添加“Microsoft 安全密码（EAP-MSCHAP v2）”，同时选中“Microsoft 加密的身份验证版本 2（MS-CHAP-v2）”与“Microsoft 加密的身份验证（MS-CHAP）”复选框，如果允许 VPN 用户更改密码，可以选中“用户可以在密码过期后更改密码”复选框，如图 16-229 所示。

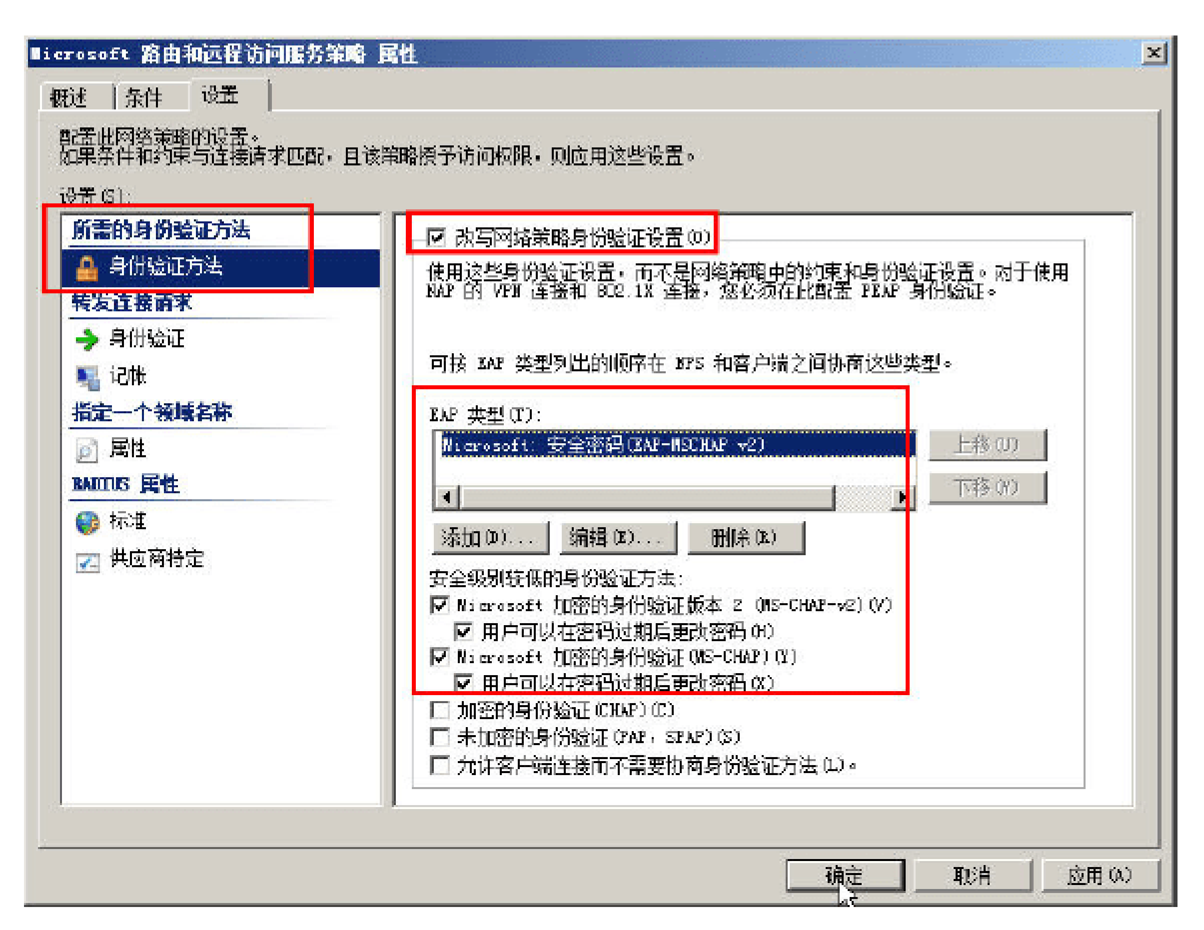


图 16-229 改写网络策略身份验证设置

设置完成后，单击“确定”按钮。

16.7.8 为 SSTP VPN 服务器创建防火墙规则

最后，还需要创建网站发布规则（发布证书服务器到 Internet）、创建网络访问规则（允许 VPN 客户端访问“内部”），下面介绍主要步骤。

01 在 Forefront TMG 控制台的“防火墙策略”中创建“网站发布规则”，在“欢迎使用新建 Web 发布规则向导”对话框中，设置规则名称为“发布证书服务器到 192.168.254.10”，如图 16-230 所示。

02 在“内部发布详细信息”对话框中，选中“使用计算机名称或 IP 地址连接到发布的服务器”，并且设置服务器的 IP 地址为 192.168.254.10，如图 16-231 所示。

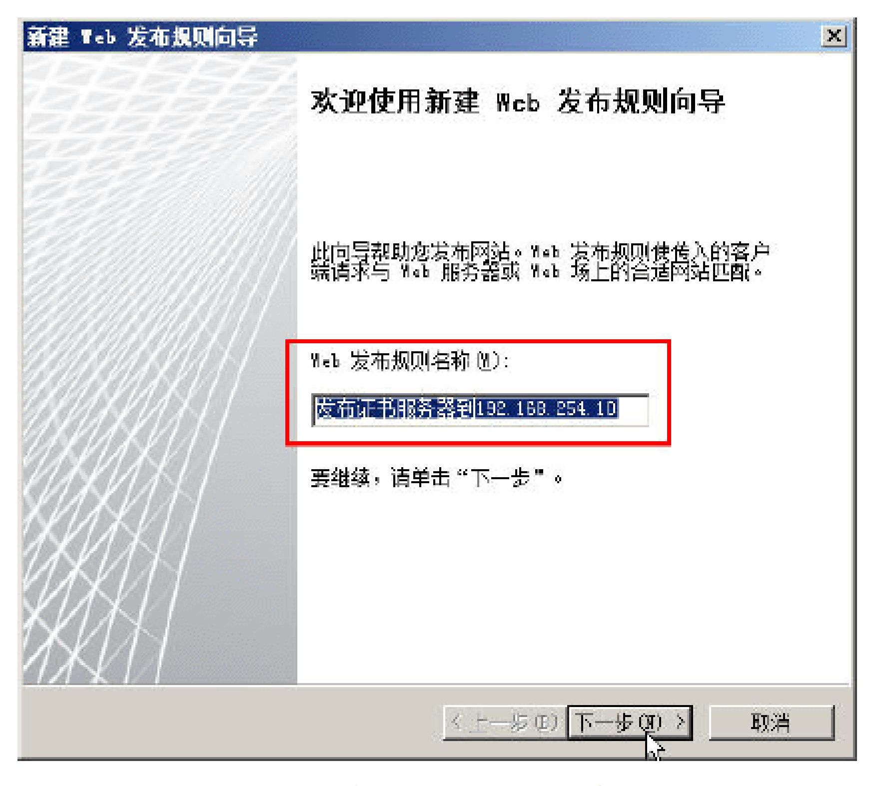


图 16-230 发布 Web 服务器

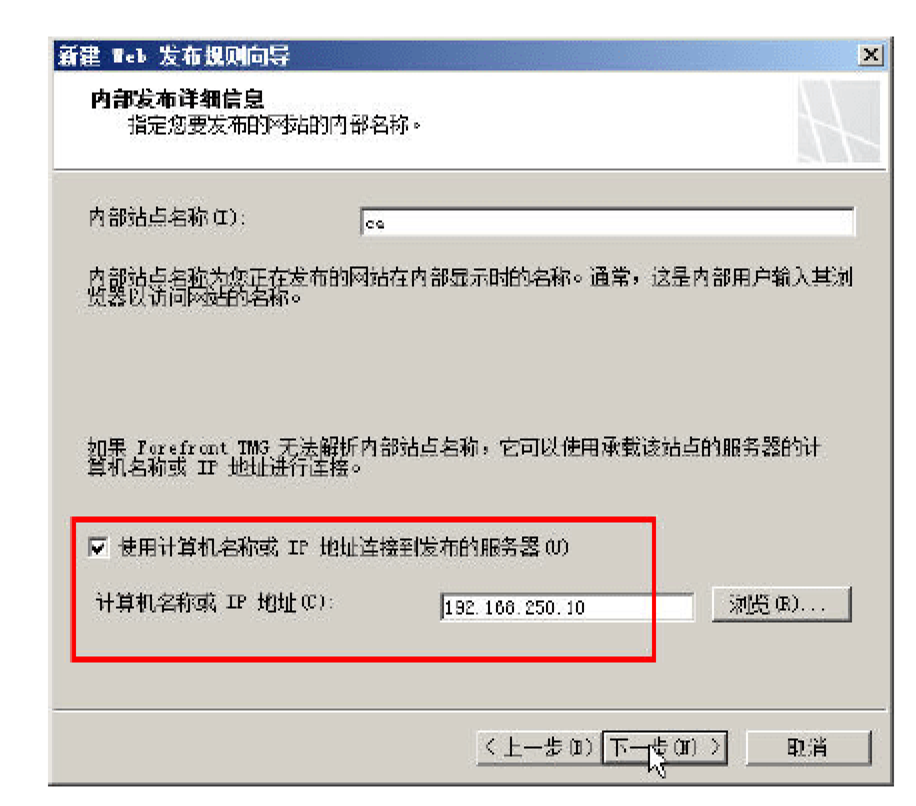


图 16-231 指定服务器 IP 地址

03 在“公共名称细节”对话框中，在“公用名称”文本框中输入“ca.msft.com”，如图 16-232 所示。

04 在“选择 Web 侦听器”对话框中，选择“Web Detect”选项，如图 16-233 所示。

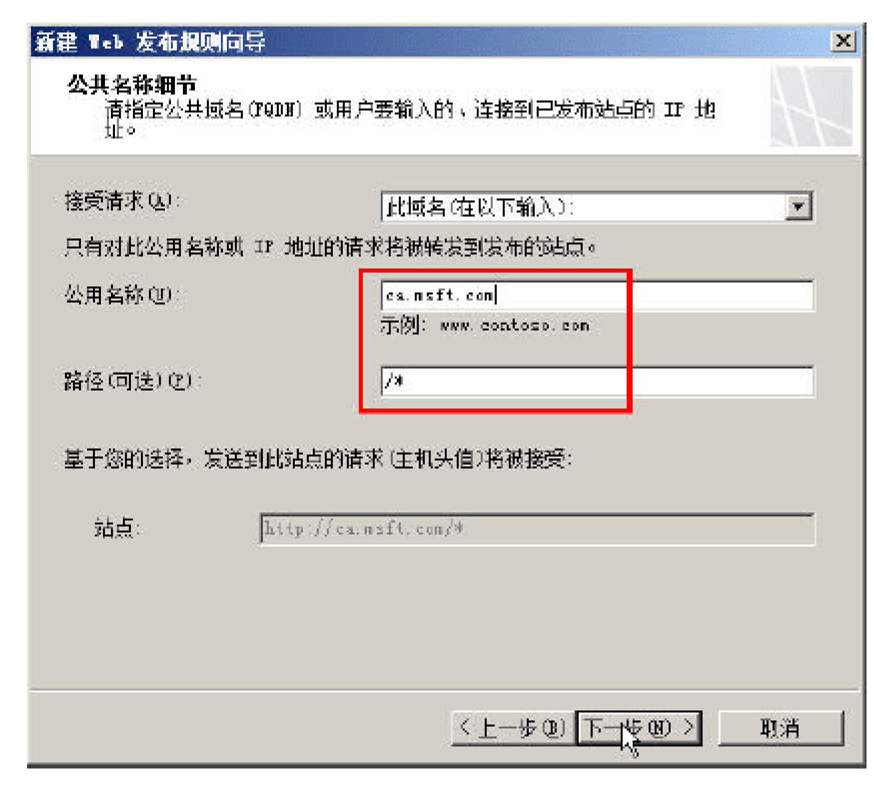


图 16-232 指定公用名称

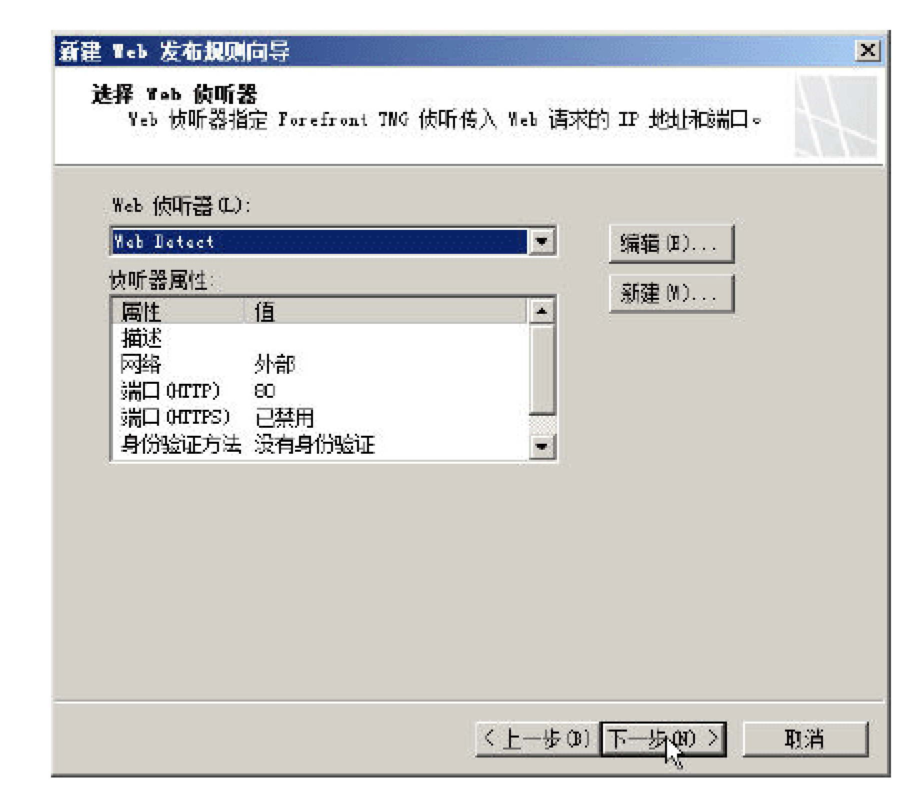


图 16-233 选择 Web 侦听器

05 创建完 Web 服务器发布规则后，接下来创建访问规则，并设置访问规则名称为“允许 VPN 访问内部”。

06 在“访问规则源”对话框中，添加“VPN 客户端”及“被隔离的 VPN 客户端”，如图 16-234 所示。

07 在“访问规则目标”对话框中，添加“内部”，如图 16-235 所示。

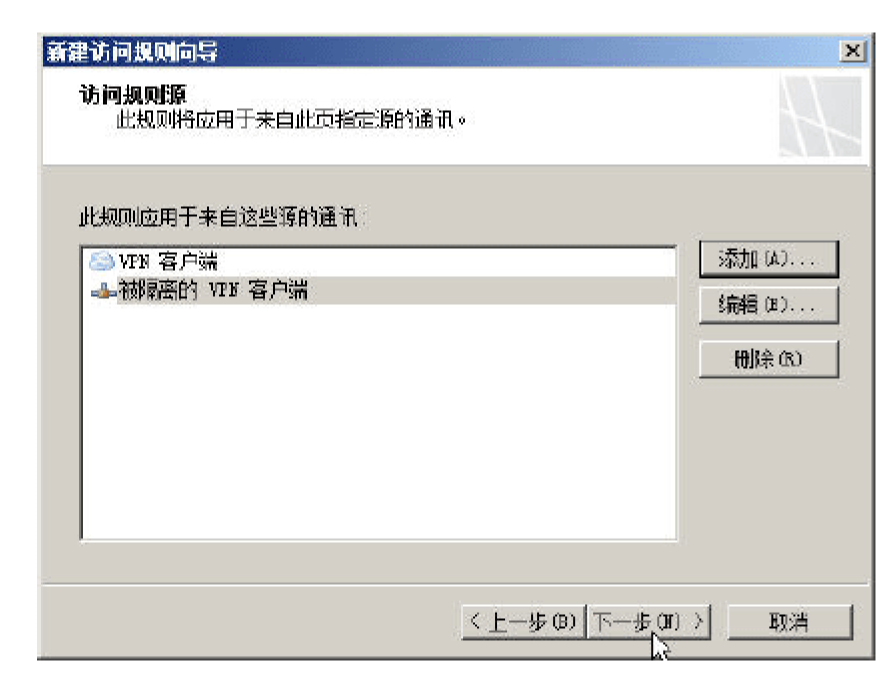


图 16-234 访问规则源

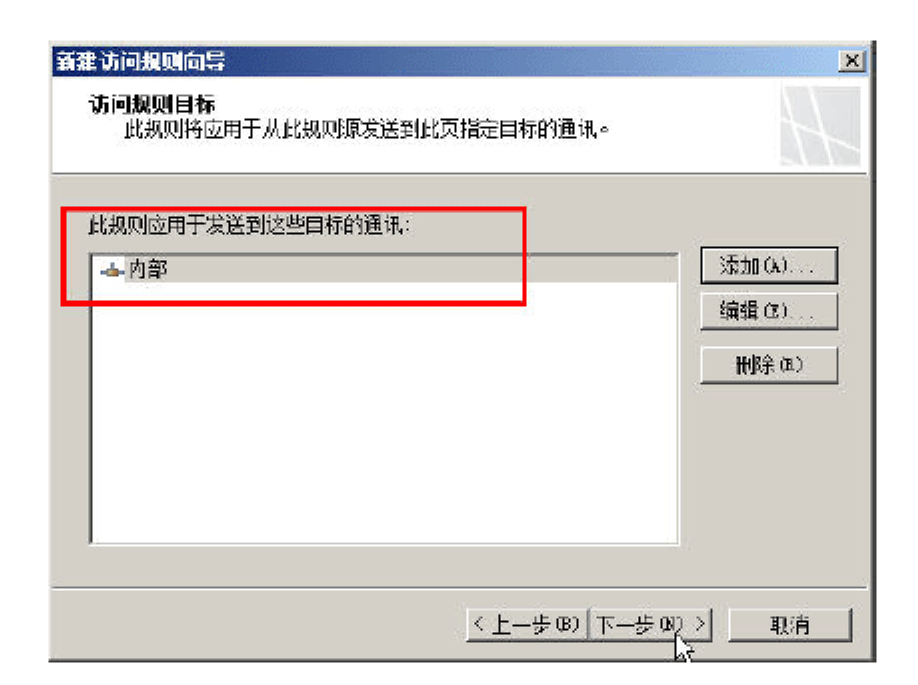


图 16-235 访问规则目标

08 创建完服务器发布规则与访问规则后，单击“应用”按钮，让设置生效，如图 16-236 所示。

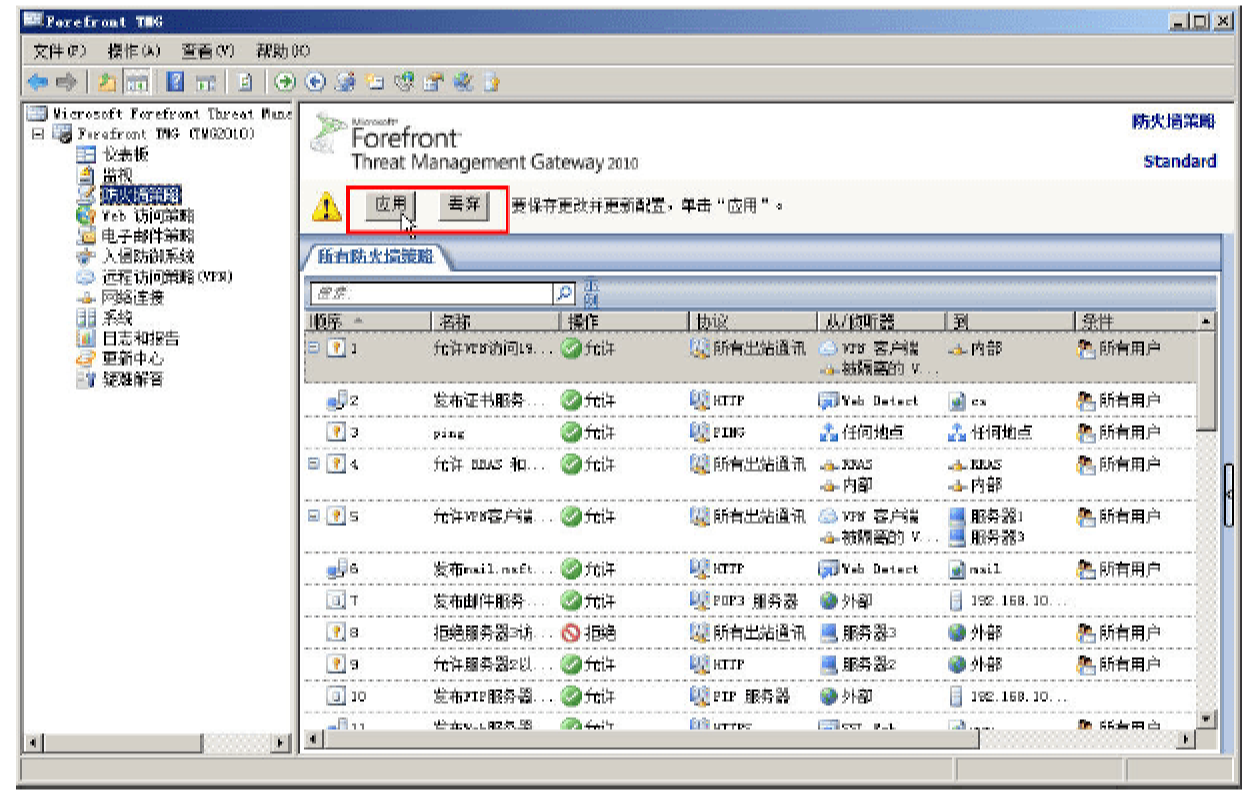


图 16-236 让设置生效

16.7.9　基于 SSTP 的 VPN 客户端的测试

在 Windows 7 的客户端计算机上，使用 SSTP 协议呼叫 VPN 服务器，主要内容包括：

- 信任根证书颁发机构。
- 创建 VPN 拨号连接并以 SSTP 协议呼叫 VPN 服务器。

这些内容，在第 15 章中有过介绍，下面介绍主要步骤。

01 在 Windows 7 客户端，设置 IP 地址为 202.206.197.121，如图 16-237 所示。

02 修改 c:\windows\system32\drivers\etc\hosts 文件，添加 ca.msft.com 与 sstp.msft.com 到 202.206.197.125，如图 16-238 所示。

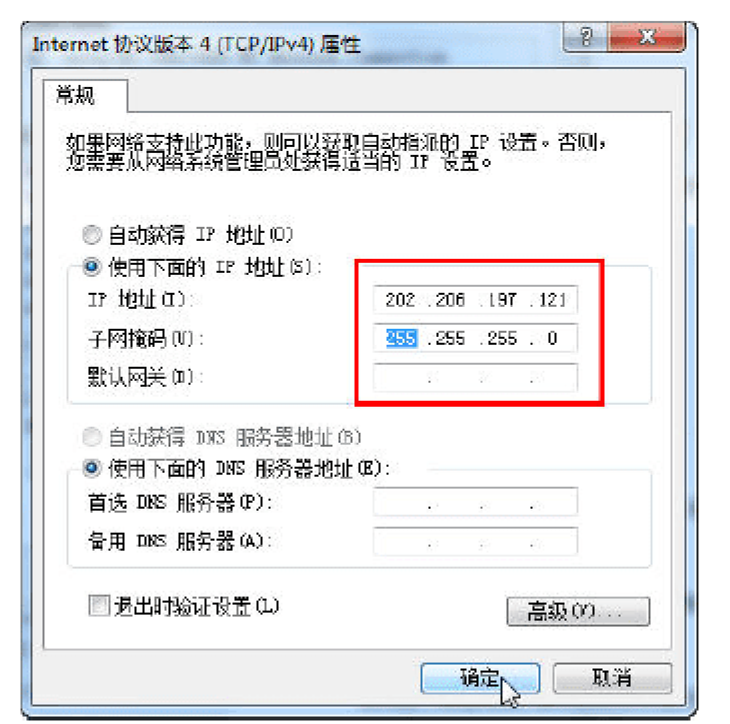


图 16-237　设置 IP 地址

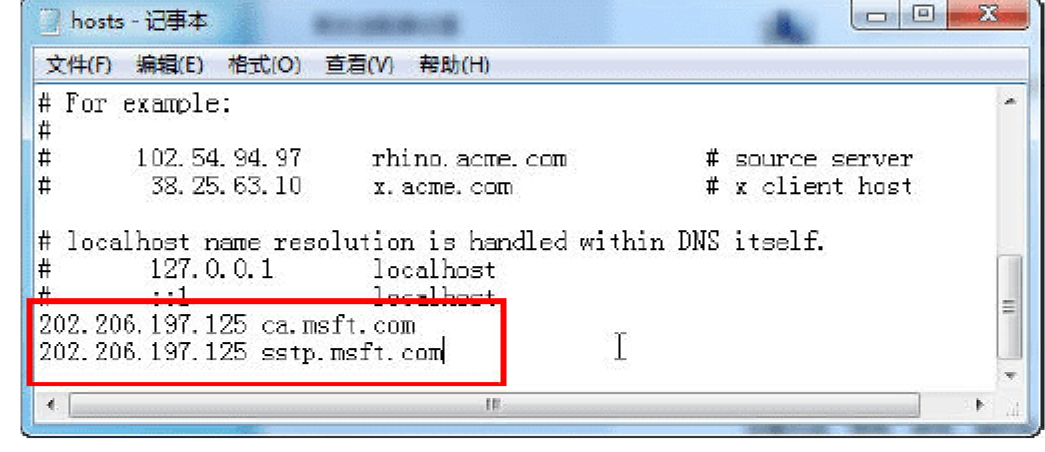


图 16-238　修改 hosts 文件

03 登录 http://ca.msft.com/certsrv 并“下载 CA 证书”（如图 16-239 所示），然后将其导入到“本地计算机存储中”，如图 16-240 所示。

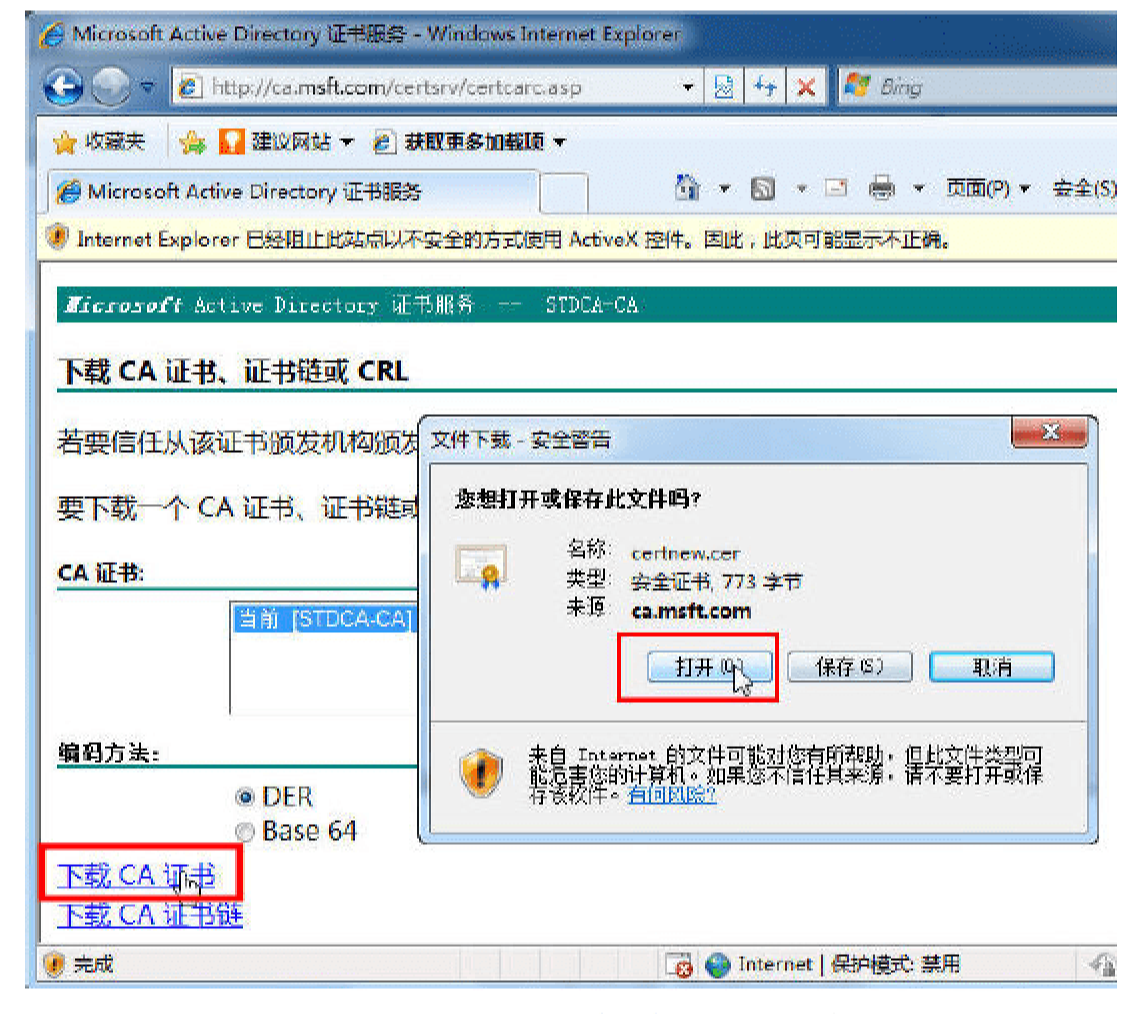




图 16-239　下载并保存 CA 证书

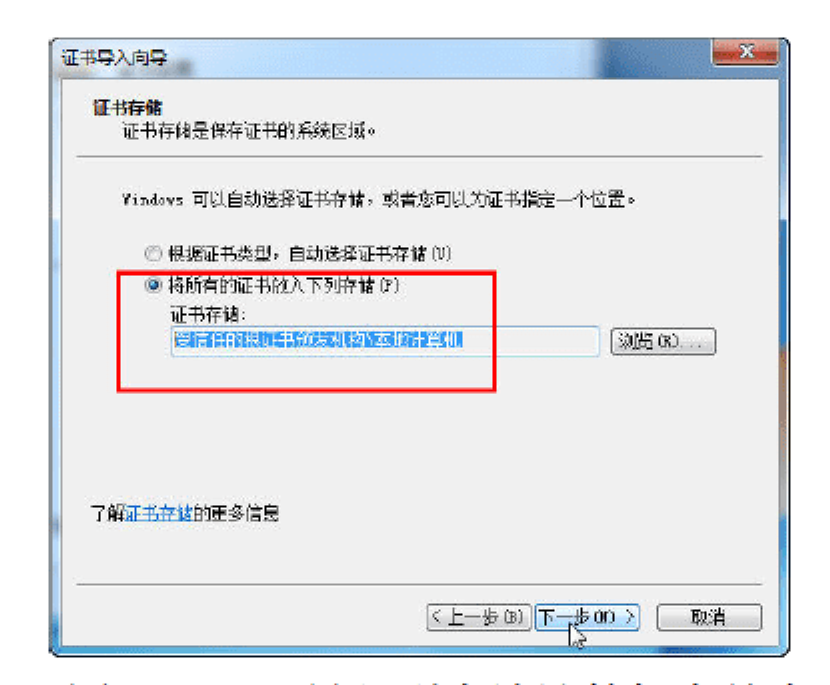


图 16-240　导入到本地计算机存储中

04 创建 VPN 连接，指定 VPN 服务器的地址为 sstp.msft.com，如图 16-241 所示。

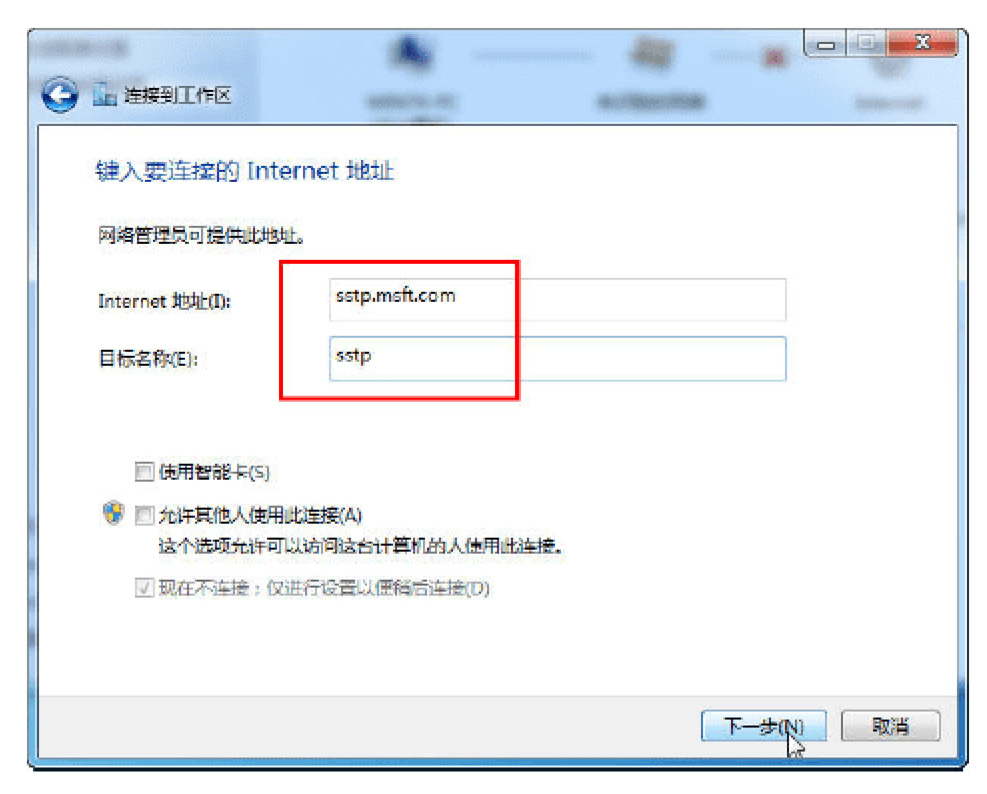
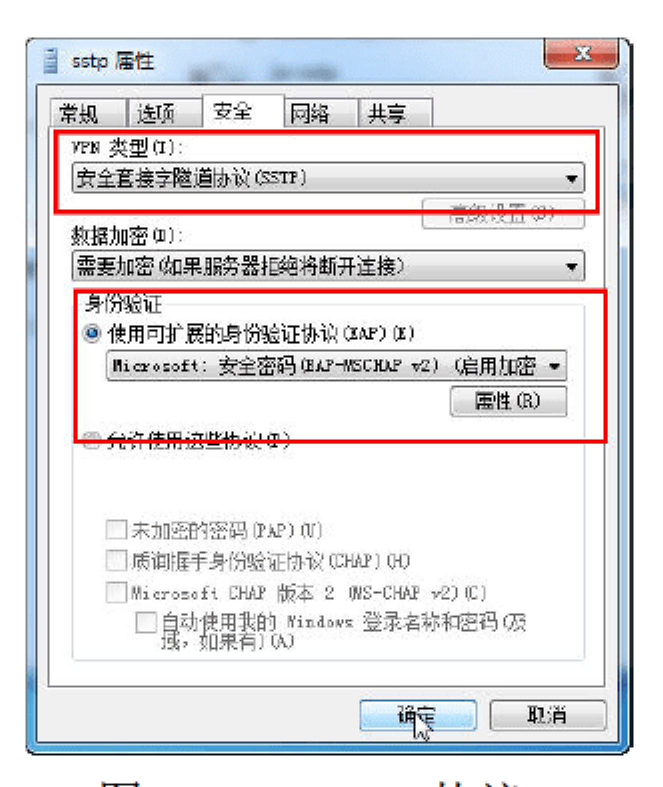


图 16-241　指定 VPN 服务器的域名

05 创建完 VPN 服务器后，修改 VPN 服务器的属性，打开“安全”项选卡，在“VPN 类型”下拉列表中选择“安全套接字隧道协议（SSTP）”选项，并在“身份验证”选项组中选中“使用可扩展的身份验证协议”单选按钮（如图 16-242 所示）或选中“允许使用这些协议”单选按钮，如图 16-243 所示（两者选一即可）。



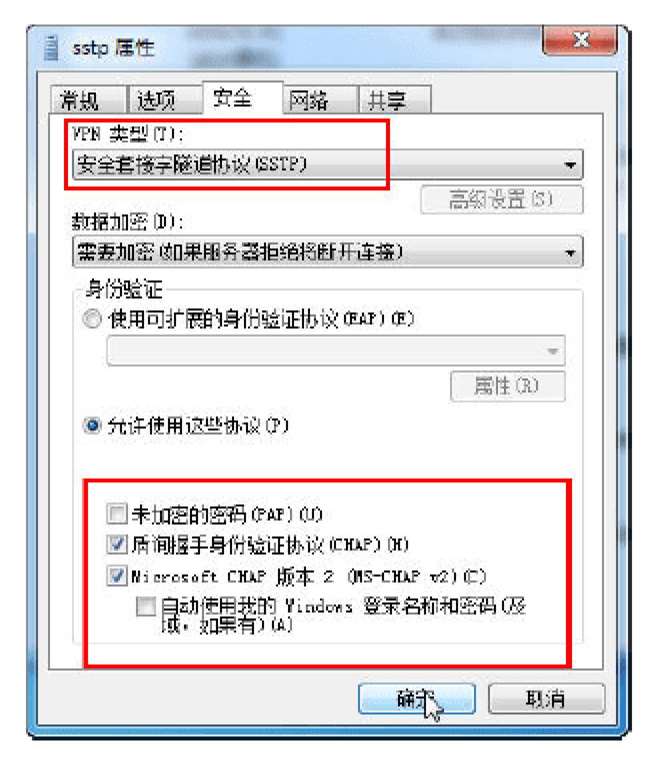



图 16-242　EAP 协议　　　　图 16-243　使用 MS-CHAP v2 协议

06 设置完成之后，拨号 VPN 服务器，即可以以 SSTP 协议连接到 VPN 服务器，如图 16-244 所示。

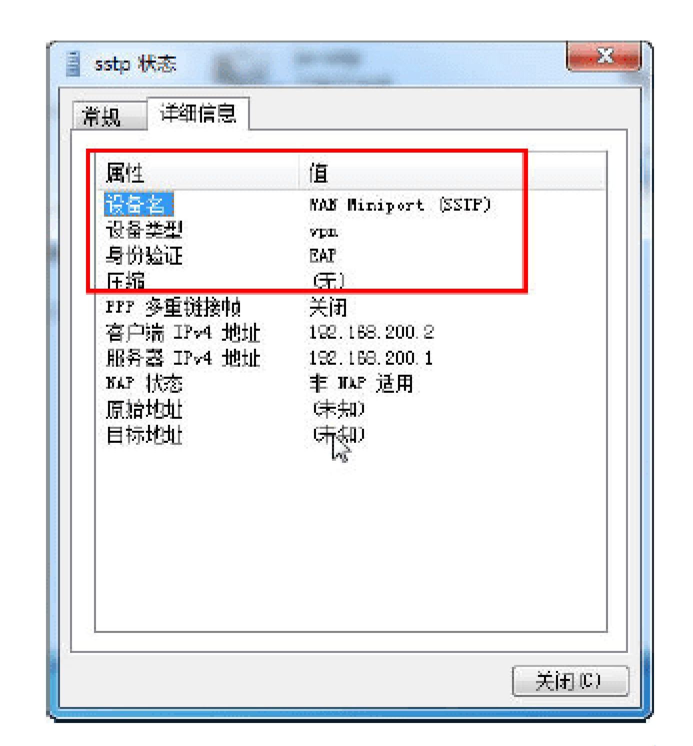


图 16-244　以 SSTP 协议呼叫 VPN 服务器成功

16.7.10　常见故障及解决方法

在本次案例中，可能会出现的故障有：

（1）错误 649：VPN 用户没有拨入权限，错误如图 16-245 所示。

出现这个错误时，需要修改 VPN 服务器端，将 VPN 用户的“拨入属性”设置为“允许拨入”即可。

（2）错误 812：RAS/VPN 服务器上的配置策略阻止，如图 16-246 所示。

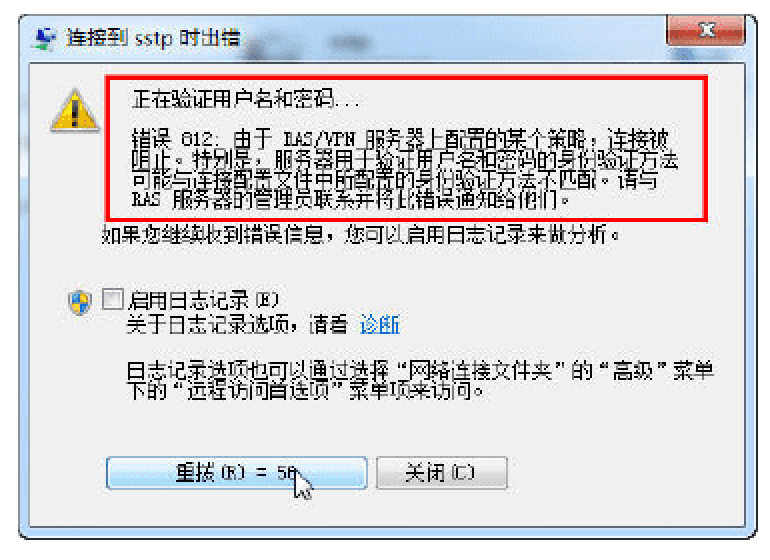


图 16-245　VPN 用户没有拨入权限

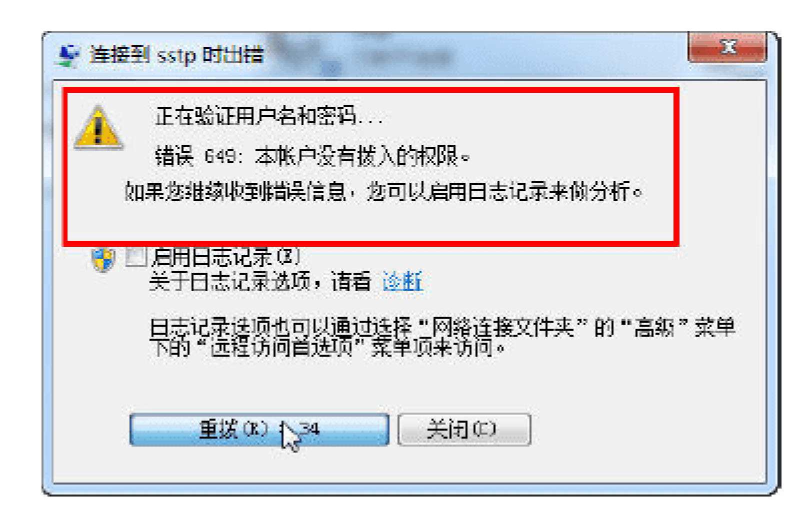


图 16-246　错误 812

出现这个错误是由于在 VPN 服务器上，没有配置 NPS 服务器，如果要解决这个问题，可参照“16.7.7 修改 NPS 访问策略”一节进行设置。

（3）错误 0x80092013：吊销服务器已脱机，如图 16-247 所示。

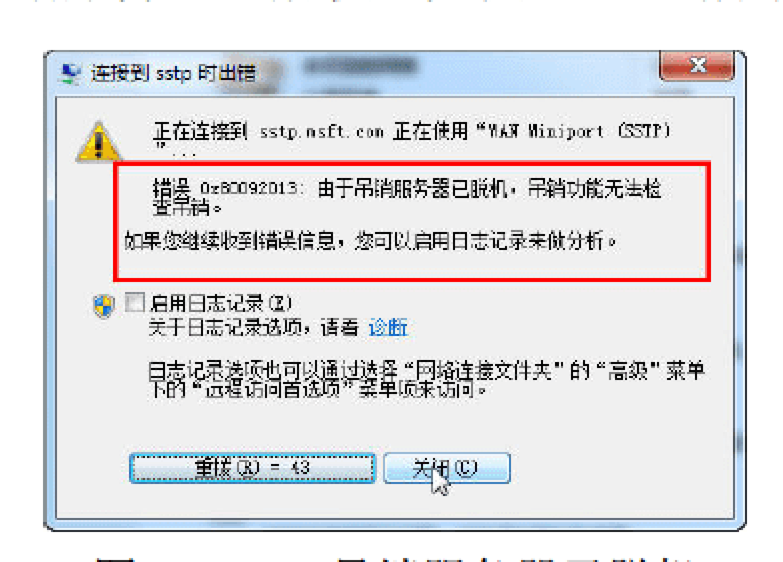


图 16-247　吊销服务器已脱机

出现这个错误时，可能的原因是：

- 证书服务器已经脱机，或者证书服务器所属的 Web 服务器没有启动。
- Forefront TMG 没有将“证书服务器”发布到 Internet。

可参照“16.7.3 配置证书服务器”一节内容进行设置。